Galois'n teoria polynomien ratkeavuudesta

Wille Lehtomäki

HELSINGIN YLIOPISTO — HELSINGFORS UNIVERSITET — UNIVERSITY OF HELSINKI

Tiedekunta/Osasto — Fakultet/Sektion — Faculty	Laitos — Institution — Department
Matemaattis-luonnontieteellinen	Matematiikan ja tilastotieteen laitos

Tekijä — Författare — Author
Wille Lehtomäki

Työn nimi — Arbetets titel — Title

Galois'n teoria polynomien ratkeavuudesta

Oppiaine — Läroämne — Subject
Matematiikka

Työn laji — Arbetets art — Level	Aika — Datum — Month and year	Sivumäärä — Sidoantal — Number of pages
Pro gradu -tutkielma	Joulukuu 2017	66 s.

Tiivistelmä — Referat — Abstract

Työn päätavoitteena on osoittaa viidennen asteen polynomiyhtälön ratkaisukaavan mahdottomuus. Ratkaisukaava on mahdollista muodostaa vain polynomeille, jotka ovat juurtamalla ratkeavia. Juurtamalla ratkeavan polynomin kukin juuri voidaan ilmaista kerroinkunnan alkioiden muodostamana päättyvänä lausekkeena, joka käyttää vain kunnan laskutoimituksia ja juurenottoa. Työn lähtökohdaksi otetaan kuntien laajennukset ja ennen kaikkea polynomin kerroinkunnan laajennukset polynomin juurilla. Kun kerroinkuntaa laajennetaan juuri kerrallaan, syntyy useiden sisäkkäisten kuntalaajennusten torni, jonka huipulla on polynomin kaikki juuret sisältävä polynomin juurikunta.

Galois'n teorian keskeisimpiä työvälineitä ovat automorfismit eli kunnan isomorfismit itselleen. Sellaiset laajennuskunnan automorfismit, jotka kiinnittävät laajennuksen lähtökunnan, muodostavat laajennuksen Galois'n ryhmän. Myös polynomille on mahdollista määritellä Galois'n ryhmä: polynomin Galois'n ryhmä on sen juurikunnan Galois'n ryhmä polynomin kerroinkunnan suhteen. Osoittautuu, että kukin Galois'n ryhmän alkio on samaistettavissa jonkin polynomin juurten permutaation kanssa, joten Galois'n ryhmä on siis aina symmetrisen ryhmän aliryhmä.

Työn loppupuolella keskiöön nousevat juurilaajennukset eli kunnan laajennukset kunnan alkioiden juurroksilla. Kun sopivaan juurilaajennukseen sovelletaan kuudennessa luvussa todistettavaa Galois'n teorian peruslausetta, osoittautuu, että juurtamalla ratkeavan polynomin Galois'n ryhmästä löytyy aina tietty sisäinen rakenne, jota kutsutaan ratkeavuudeksi.

Viimeisessä luvussa osoitetaan, että polynomin Galois'n ryhmän ratkeavuus on välttämätön ja riittävä ehto polynomin juurtamalla ratkeavuudelle. Viiden ja sitä useamman alkion symmetrinen ryhmä ei kuitenkaan ole ratkeava, mutta on olemassa polynomeja, joiden Galois'n ryhmä se on. Näin ollen polynomeille, joiden aste on viisi tai sitä korkeampi, ei ole mahdollista muodostaa yleistä ratkaisukaavaa. Työn päättää esimerkki viidennen asteen polynomista, joka ei ole juurtamalla ratkeava.

Avainsanat — Nyckelord — Keywords
Kuntalaajennukset, Galois'n ryhmä, ratkeavuus

Säilytyspaikka — Förvaringsställe — Where deposited
Kumpulan tiedekirjasto

Muita tietoja — Övriga uppgifter — Additional information

Sisältö

Luku 1

Johdanto

Toisen asteen yhtälön ratkaisukaava on monille tuttu jo koulumatematiikasta, mutta vähemmän tunnettua on, että vastaavanlainen kaava voidaan muodostaa myös kolmannen ja neljännen asteen yhtälöille. Kolmannen asteen yhtälön ratkaisukaava on kuitenkin huomattavan pitkä ja monimutkainen, ja neljännen asteen on vielä sitäkin hankalampi. Viidennen ja sitä korkeamman asteen yhtälöiden kohdalla käy lopulta niin, että vastaavanlaista yleistä ratkaisukaavaa ei edes ole mahdollista muodostaa. On kuin algebralta loppuisivat voimat neljännen asteen jälkeen, ja tässä työssä käsiteltävä Galois'n teoria selittää syyn.

Työn lähestymistapa yhdistelee polynomien, ryhmien ja kuntien teoriaa. Tunnetuiksi oletetaan tiedot niistä siinä laajuudessa, missä ne esitetään esimerkiksi teoksessa [5]. Työn lähtökohdaksi otetaan kuntien laajennukset, mutta luvussa 6 esiteltävä Galois'n teorian peruslause yhdistää kuntalaajennukset niitä vastaavien juurten permutaatioiden kanssa. Näitä juurten muodostamia permutaatioryhmiä kutsutaan Galois'n ryhmiksi, ja niiden sisäinen rakenne antaa kaiken tarvittavan tiedon polynomien ratkeavuudesta.

Rationaali- ja reaalikertoimiset polynomit ovat olleet keskeisessä asemassa algebran historiassa, mutta työssä esiteltävä nykyaikainen Galois'n teoria pätee myös yleisille ryhmille ja kunnille. Viimeisessä luvussa annetaan konkreettinen esimerkki viidennen asteen rationaalikertoimisesta polynomista, jota ei voi ratkaista ratkaisukaavalla. Tällainen polynomi ei siis toisin sanottuna ole juurtamalla ratkeava.

Määritelmä 1.1. Polynomi on *juurtamalla ratkeava*, jos sen jokainen juuri on mahdollista johtaa äärellisellä määrällä askelia polynomin kertoimista käyttäen vain kunnan laskutoimituksia ja n:nen juuren ottoa.

Esimerkiksi toisen asteen polynomiyhtälö $ax^2 + bx + c = 0$, missä $a, b, c \in \mathbb{Q}$, on juurtamalla ratkeava, sillä käyttämällä kunnan $\mathbb{Q}$ laskutoimituksia ja neliöjuuren ottoa

kertoimiin a, b, c voidaan polynomin juuret ilmaista muodossa

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Juuret voidaan ilmaista tässä muodossa silloinkin, kun yhtälön diskriminantti $b^2 - 4ac$ on nollaa pienempi eikä yhtälöllä ole reaalisia ratkaisuja. Tällöin juuret ovat kompleksisia eli ilmaistavissa imaginääriyksikön i avulla.

Tämän tunnetun ratkaisukaavan löytäminen edellytti kuitenkin tuhansien vuosien matemaattista kehitystä, joka alkoi yksinkertaisista käytännön ongelmista ja eteni vähitellen korkeampiasteisten yhtälöiden tarkasteluun. Myös viidennen asteen yhtälön yleistä ratkaisua etsittiin kuumeisesti aina 1800-luvulle asti, jolloin se lopulta osoitettiin mahdottomaksi.

1.1 Historiaa

Algebra on historiansa aikana edennyt mekaanisesta laskentaopista teoriaan ja formalismiin. Varhaisimmat toisen asteen yhtälön ratkaisut ovat peräisin noin vuodelta 2000 eKr. babylonialaisista kivitauluista. Niissä ratkaistut ongelmat ovat lähtöisin käytännön tilanteista, ja tauluissa esitetty ratkaisutapa on vahvan proseduraalinen. Myös kreikkalaiset matemaatikot (n. 500 eKr. – 300 jKr.) jatkoivat geometrisen painotuksensa vuoksi varsin käytännönläheisellä linjalla, mutta kreikkalaiset kuitenkin oivalsivat todistamisen ja deduktiivisen päättelyn merkityksen.

Itsenäiseksi matematiikan osa-alueeksi algebra alkoi todella kehittyä vasta arabialaisen kulttuurin kulta-aikana (n. 800–1200 jKr.). Arabialaiset matemaatikot kehittivät erityisesti algebran formalismia, mikä mahdollisti algebran irtautumisen käytännön ongelmien asettamista rajoitteista. Samalla kehitettiin myös yleisiä yhtälönratkaisumenetelmiä, jotka kuitenkin perusteltiin edelleen kreikkalaisilta opitulla tavalla geometrisesti. Myös arabialaisten löytämä ratkaisu kolmannen asteen yhtälölle oli geometrinen.

Algebrallinen ratkaisu kolmannen ja pian myös neljännen asteen yhtälölle löydettiin renessanssiajan Italiassa. Ratkaisut saatiin kuitenkin lähinnä manipuloimalla annettua yhtälöä erilaisilla sijoituksilla ja muilla tekniikoilla, joten ratkaisuilla ei ollut vahvaa teoreettista pohjaa. Pian kuitenkin osoittautui, että vastaavat tekniset manipulaatiot eivät tuottaneet toivottuja tuloksia viidennen asteen yhtälön kohdalla, jolloin syntyi tarve lähestyä yhtälönratkaisua ja polynomeja teoreettisemmasta näkökulmasta.

Erityisesti Joseph-Louis Lagrangen (1736–1813) ja Carl Friedrich Gaussin (1777–1855) tutkimukset polynomien juurten muodostamien permutaatioiden ja funktioiden saralla edistivät alaa siinä määrin, että 1800-luvun alussa Niels Henrik Abel (1802–1829) ja Paolo Ruffini (1765–1822) kykenivät toisistaan riippumatta todistamaan viidennen yhtälön

ratkaisukaavan mahdottomuuden. Kumpikaan todistuksista ei kuitenkaan esittänyt kriteeriä, jolla jokin annettu viidennen asteen yhtälö voitaisiin näyttää ratkeamattomaksi.

Ratkeamattomuuden kriteerin löysi ranskalainen Evariste Galois (1811–1832) pian Abelin ja Ruffinin todistusten jälkeen. Galois tutki polynomin juurten permutaatioita käyttäen algebrallisia rakenteita, joiden pohjalta syntyi myöhemmin nykyinen ryhmien teoria. Galois'n ratkaisu oli kuitenkin niin monimutkainen ja epäselvä, että Galois'n kuoltua 20-vuotiaana kaksintaistelussa hänen ratkaisunsa sai enemmän huomiota vasta Joseph Liouvillen (1809–1882) julkaistua sen vuonna 1846.

Osittain juuri Galois'n alkuperäisen menetelmän hankaluudesta johtuen nykyaikainen Galois'n teoria ei ota lähtökohdakseen polynomin juurten permutaatioita, vaan pikemminkin polynomin kerroinkunnan laajennukset. Tämäkin työ pohjautuu pitkälti tähän Emil Artinin (1898–1962) teoksessa [1] esittämään kuntateoreettiseen lähestymistapaan.

Luku 2

Kuntalaajennukset

Galois'n teoria lähestyy juurtamalla ratkeavuuden ongelmaa laajentamalla polynomin kerroinkuntaa polynomin juurilla. Minkä tahansa viidennen asteen rationaalikertoimisen polynomiyhtälön kaikki juuret ovat algebran peruslauseen nojalla kunnassa $\mathbb{C}$, joten periaatteessa polynomin kerroinkunnan $\mathbb{Q}$ voisi suoraan laajentaa kunnaksi $\mathbb{C}$. Näin holtiton laajentaminen suoraan kaikki juuret sisältävään kuntaan $\mathbb{C}$ ei kuitenkaan kerro polynomin *juurtamalla ratkeavuudesta*, sillä pelkkä juuren olemassaolo ei takaa sitä, että se olisi ilmaistavissa juurilausekkein.

Tavoitteenamme onkin laajentaa polynomin kerroinkuntaa hallitusti ja usein pienin väliaskelein. Näin menetellen saadaan kustakin välilaajennuksesta enemmän tietoa, ja myöhemmin osoitetaan, että polynomin juurtamalla ratkeavuus on pääteltävissä sisäkkäisten kuntalaajennusten jonojen rakenteesta.

2.1 Yleiset laajennukset

Kuntalaajennukset määritellään alikunnan käsitteen avulla. Kunnan K *alikunta* on mikä tahansa kunnan osajoukko, joka on suljettu yhteenlaskun ja kertolaskun sekä niiden käänteistoimitusten suhteen. Mikä tahansa alikunta on luonnollisesti itsekin aina kunta.

Määritelmä 2.1. Kunnan K *laajennus* L/K on mikä tahansa kunta L, joka sisältää kunnan K alikuntanaan.

Laajennuksessa L/K kuntaa K kutsutaan usein *lähtökunnaksi* ja kuntaa L *laajennuskunnaksi*.

Lähtökunnan näkökulmasta ne laajennuskunnan alkiot, jotka eivät ole lähtökunnassa, ovat hieman tuntemattomia. Lähtökunnan laskutoimitukset on määritelty vain lähtökunnan alkioille, eivätkä ne siten ota kantaa laajennuskunnan alkioihin. Siksi onkin

hyödyllistä, että laajennuskunta muodostaa vektoriavaruuden, jossa lähtökunnan alkiot ovat skalaareja ja laajennuskunnan alkiot vektoreita. Tällöin laajennuksen alkioita osataan käsitellä vektoriavaruuden laskutoimituksilla, ja koko laajennus saa konkreettisemman rakenteen ennen kaikkea vektoriavaruuden kannan ja dimension kautta.

Määritelmä 2.2. Kuntalaajennuksen L/K *aste* $[L : K]$ on kunnan L dimensio K-vektoriavaruutena. Jos laajennuksen aste on äärellinen, sanotaan laajennuksen olevan äärellinen.

Laajennuksen asteen voi ajatella kuvaavan kuntalaajennuksen monimutkaisuutta: mitä suurempi on kuntalaajennuksen aste, sitä enemmän resursseja tarvitaan laajennuskunnan alkioiden käsittelyyn.

Esimerkki 2.3. Tarkastellaan laajennusta $\mathbb{C}/\mathbb{R}$. Joukko $\{1, i\}$ muodostaa tunnetusti $\mathbb{R}$-vektoriavaruuden $\mathbb{C}$ kannan, joten laajennuksen $\mathbb{C}/\mathbb{R}$ aste on 2, ja se on siten äärellinen.

Galois'n teoria ei kuitenkaan tyydy laajentamaan tarkasteltavaa kuntaa vain kerran. Sen sijaan pyrkimyksenä onkin laajentaa kuntia askel kerrallaan määrittelemällä useita sisäkkäisiä kuntalaajennuksia, joissa kukin uusi kunta laajentaa edellistä. Tällöin puhutaan laajennuksen välikunnista.

Määritelmä 2.4. Olkoon L kunnan K laajennus. Kuntaa M sanotaan laajennuksen L/K *välikunnaksi*, jos $K \subset M \subset L$.

Varsinkin englanninkielisessä kirjallisuudessa tällaisia sisäkkäisiä laajennuksia nimitetään usein laajennusten muodostamaksi *torniksi*. Tästä syystä seuraavaa tulosta kutsutaan usein tornilauseeksi (engl. *Tower Law*).

Lause 2.5. *Olkoon $K \subset M \subset L$ jono kuntia. Tällöin $[L : K] = [L : M] \cdot [M : K]$.*

Todistus. Olkoon $\{a_i\}_{i \in I}$ laajennuksen M/K kanta ja $\{b_j\}_{j \in J}$ laajennuksen L/M kanta. Lauseen todistamiseksi riittää osoittaa, että joukko $S = \{a_i b_j : i \in I, j \in J\}$ on laajennuksen L/K kanta. (Joukon S indeksöinnissä sallitaan tilanne $a_i b_j = a_k b_l$, kun $i \neq k$ tai $j \neq l$, mutta todistuksessa osoitetaan joukon S olevan vapaa, joten jokaisella joukon S alkiolla on yksikäsitteinen esitys $a_i b_j$, missä $i \in I$ ja $j \in J$.)

Osoitetaan ensin, että joukko S virittää K-vektoriavaruutena kunnan L. Oletetaan, että $\alpha \in L$. Alkio α on laajennuksen L/M alkio, joten $\alpha = \sum_{j \in J} m_j b_j$, missä $m_j \in M$ kaikilla $j \in J$. Jokainen m_j on kuitenkin laajennuksen M/K alkio, joten $m_j = \sum_{i \in I} k_{ij} a_i$, missä $k_{ij} \in K$ kaikilla $i \in I, j \in J$. Näin ollen

$$\alpha = \sum_{j \in J} m_j b_j = \sum_{j \in J} \Big(\sum_{i \in I} k_{ij} a_i \Big) b_j = \sum_{i,j} k_{ij} a_i b_j.$$

Osoitetaan vielä, että S on vapaa. Oletetaan, että $\sum_{i,j} k_{ij}a_ib_j = 0$, missä $k_{ij} \in K$ kaikilla $i \in I, j \in J$. Tällöin

$$\sum_{i,j} k_{ij}a_ib_j = \sum_{j\in J}\Big(\sum_{i\in I} k_ia_i\Big)b_j = 0.$$

Joukko $\{b_j\}_{j\in J}$ on kuitenkin vapaa, joten on oltava $\sum_{i\in I} k_{ij}a_i = 0$ kaikilla $j \in J$. Koska myös joukko $\{a_i\}_{i\in I}$ on vapaa, on oltava $k_{ij} = 0$ kaikilla i, j. □

Määritelmä 2.6. Olkoon L kunnan K laajennus, ja olkoon A joukko laajennuksen L alkioita.

1. *Joukon A virittämä laajennuksen L/K alilaajennus* $K(A)$ on pienin laajennuskunnan L alikunta, joka sisältää sekä kunnan K että joukon A.

2. Jos joukko $A = \{\alpha_1, \ldots, \alpha_n\}$ on äärellinen, merkitään $K(A) = K(\alpha_1, \ldots, \alpha_n)$, ja laajennuksen $K(\alpha_1, \ldots, \alpha_n)$ sanotaan olevan *äärellisviritteinen.*

3. Jos $K(A) = K(\alpha)$ jollain yksittäisellä alkiolla α, sanotaan laajennuksen olevan *yksinkertainen.*

On hyvä huomata ero laajennuksen äärellisyyden ja äärellisviritteisyyden kanssa: myöhemmin osoitetaan, että äärellinen laajennus on aina äärellisviritteinen, mutta äärellisviritteinen laajennus ei välttämättä ole äärellinen.

Esimerkki 2.7. Olkoon $\alpha \in L$. Tällöin yksinkertainen laajennus $K(\alpha)$ on määritelmällisesti pienin laajennus, joka sisältää sekä kunnan K että alkion α. Kyseessä on kunta, joten sen tulee sisältää kunnan K lisäksi sellaisten algebrallisten operaatioiden tulokset, joissa alkio α on mukana. Toisin sanoen kunnan $K(\alpha)$ tulee siis sisältää alkion α kaikki K-kertoimiset lineaarikombinaatiot.

Ei kuitenkaan ole tarpeen tyytyä pelkkään lineaarikombinaatioiden sisältymiseen kuntaan $K(\alpha)$. Seuraavassa aliluvussa osoitetaan, että jos α on jonkin K-kertoimisen polynomin juuri, niin itse asiassa jokaiselle laajennuksen $K(\alpha)$ alkiolle on olemassa yksikäsitteinen esitys alkion α potenssien K-lineaarikombinaationa.

2.2 Algebralliset laajennukset

Kuntalaajennuksen käsitteleminen vektoriavaruutena antaa laajennukselle enemmän rakennetta, mutta laajennuksen ominaisuuksien sitominen polynomien tutkimiseen vaatii

lisää apuneuvoja. Osoittautuu, että kerroinkunnan laajentaminen tarkasteltavan polynomin juurilla mahdollistaa polynomien teorian hyödyntämisen kuntalaajennusten tutkimiseen. Polynomin juuria ei kuitenkaan tarvitse tuntea täsmällisesti etukäteen – tavoitteenamme onkin selvittää polynomin ratkeavuus tarvitsematta kuitenkaan varsinaisesti ratkaista polynomia.

Määritelmä 2.8. Alkion α sanotaan olevan *algebrallinen* kunnan K suhteen, jos se on jonkin K-kertoimisen nollasta poikkeavan polynomin juuri.

Määritelmä 2.9. Olkoon L kunnan K laajennus. Laajennusta L/K sanotaan *algebralliseksi*, jos jokainen kunnan L alkio on algebrallinen kunnan K suhteen.

Alkion α algebrallisuus takaa sen olevan ainakin yhden K-kertoimisen polynomin juuri, mutta se ei estä, etteikö α voisi olla useammankin polynomin juuri. Hyödyllisimmäksi osoittautuukin tarkastella "pienintä" polynomia, jonka juuri α on.

Määritelmä 2.10. Polynomi $m(x)$ on alkion $\alpha \in L$ *minimipolynomi* kunnan K suhteen, jos seuraavat ehdot pätevät:

1. Polynomin $m(x)$ kertoimet ovat kunnassa K.
2. Polynomin $m(x)$ korkeimman asteen termin kerroin on 1.
3. Alkio α on polynomin $m(x)$ juuri.
4. Polynomin $m(x)$ aste on matalin kaikista niistä K-kertoimisista polynomeista, jotka toteuttavat ehdot 1 - 3.

Minimipolynomi määritellään *aina* tietyn kunnan suhteen. Tässä esityksessä alkion minimipolynomia kunnan K suhteen merkitään lyhyesti $m(x) \in K[x]$.

Määritelmä antaa olettaa, että alkion minimipolynomi on yksikäsitteinen. Osoitetaan, että näin todellakin on.

Lemma 2.11. *Alkion $\alpha \in L$ minimipolynomi on yksikäsitteinen.*

Todistus. Oletetaan, että alkiolla alkiolla α olisi kaksi toisistaan poikkeavaa minimipolynomia $a(x), b(x) \in K[x]$. Minimipolynomin määritelmästä seuraa, että tällöinkin on oltava $\deg(a(x)) = \deg(b(x))$, joten voidaan merkitä

$$a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_2 x + a_1 \quad \text{ja} \quad b(x) = b_n x^n + b_{n-1}x^{n-1} + \cdots + b_2 x + b_1.$$

Minimipolynomin korkeimman asteen termin kerroin on aina 1, joten $a_n = b_n = 1$. Näin ollen erotuspolynomille $(a-b)(x) \in K[x]$ pätee

$$\begin{aligned}(a-b)(x) &= a(x) - b(x) \\ &= x^n + a_{n-1}x^{n-1} + \cdots + a_2x + a_1 - (x^n + b_{n-1}x^{n-1} + \cdots + b_2x + b_1) \\ &= (a_{n-1} - b_{n-1})x^{n-1} + \cdots + (a_2 - b_2)x + (a_1 - b_1),\end{aligned}$$

joten erotuspolynomin $(a-b)(x)$ aste on $n-1$. Tiedetään kuitenkin, että $a(\alpha) = 0$ ja $b(\alpha) = 0$, joten

$$(a-b)(\alpha) = a(\alpha) - b(\alpha) = 0.$$

Alkio α on siis erotuspolynomin $(a-b)(x) \in K[x]$ juuri, vaikka erotuspolynomin aste on matalampi kuin minimipolynomien $a(x)$ ja $b(x)$ aste. Tämä on mahdotonta, joten on siis oltava $(a-b)(\alpha) = 0$. Siis $a(x) = b(x)$. □

On siis osoitettu, että *jos* minimipolynomi on olemassa, se on yksikäsitteinen. Mutta miten minimipolynomin olemassaolosta voidaan olla varmoja? Jos alkio $\alpha \in L$ on algebrallinen kunnan K suhteen, niin on olemassa ainakin jokin polynomi $f(x) \in K[x]$, jonka juuri α on. Lisäksi polynomin $f(x)$ korkeimman asteen kertoimen a_n voidaan varmistaa olevan 1 jakamalla polynomi $f(x)$ tarvittaessa kertoimella a_n. Mutta miten voidaan olla varmoja, että ei ole olemassa jotain matalampaa astetta olevaa polynomia, jonka juuri alkio α on?

Avaimeksi ongelmaan nousee polynomin jaollisuus. Jos edellä mainittu polynomi $f(x)$ on jaollinen renkaassa $K[x]$, niin on olemassa jokin matalampaa astetta oleva polynomi $g(x) \in K[x]$, jolla $f(x) = g(x)h(x)$ jollain $h(x) \in K[x]$ ja lisäksi $g(\alpha) = 0$. Mutta mikäli myös polynomi $g(x)$ on jaollinen, voidaan sekin jakaa matalampaa astetta oleviin tekijöihin, joista ainakin toisella on juuri α. Tätä prosessia voidaan siis jatkaa niin kauan, kunnes löydetään jaoton polynomi, jonka juuri α on. Osoitetaan nyt täsmällisesti, että minimipolynomi onkin väistämättä aina jaoton. Lisäksi näytetään, että minimipolynomi jakaa minkä tahansa polynomin, jonka jokin juuri on α.

Lause 2.12. *Oletetaan, että alkio α on algebrallinen kunnan K suhteen. Tällöin alkion α minimipolynomi kunnan K suhteen on jaoton polynomirenkaassa $K[x]$, ja se jakaa kaikki nollasta poikkeavat renkaan $K[x]$ polynomit, joiden juuri α on.*

Todistus. Oletetaan, että alkion α minimipolynomi $m(x) \in K[x]$ ei olisikaan jaoton renkaassa $K[x]$, jolloin siis $m(x) = f(x)g(x)$ joillakin polynomeilla $f(x), g(x) \in K[x]$, joiden asteet ovat pienempiä kuin minimipolynomin $m(x)$ aste. Nyt

$$f(\alpha)g(\alpha) = m(\alpha) = 0,$$

joten joko $f(\alpha) = 0$ tai $g(\alpha) = 0$, sillä koska K on kunta, rengas $K[x]$ on kokonaisalue. Kummassakin tapauksessa alkio α olisi siis jonkin sellaisen polynomin juuri, jonka aste on pienempi kuin polynomin $m(x)$ aste. Tämä on kuitenkin mahdotonta, sillä polynomi $m(x)$ oletettiin alkion α minimipolynomiksi. Minimipolynomi $m(x)$ on siis jaoton.

Oletetaan seuraavaksi, että $h(x) \in K[x]$ on jokin polynomi, jonka juuri α on. Polynomien jakoyhtälön mukaan on olemassa polynomit $q(x), r(x) \in K[x]$, joille pätee

$$h(x) = q(x)m(x) + r(x)$$

ja $\deg(r(x)) < \deg(m(x))$. Nyt kuitenkin

$$0 = h(\alpha) = q(\alpha) \cdot 0 + r(\alpha) = r(\alpha),$$

joten alkio α on myös polynomin $r(x)$ juuri. Polynomi $r(x)$ on kuitenkin pienempää astetta kuin alkion α minimipolynomi $m(x)$, joten polynomin $r(x)$ on oltava nollapolynomi. Siis $h(x) = q(x)m(x)$ eli $m(x)$ jakaa polynomin $h(x)$. □

Edellisen lauseen tärkeyttä ei voi liiaksi korostaa. Sen ensimmäinen sovellus löytyy jo seuraavasta lauseesta, joka antaa algebrallisten laajennusten alkioille erittäin hyödyllisen esitysmuodon. Osoitetaan ensin aputulos.

Lemma 2.13. *Olkoon $K(\alpha)$ kunnan K yksinkertainen laajennus. Jokainen laajennuksen $K(\alpha)$ alkio voidaan esittää muodossa $f(\alpha)/g(\alpha)$, missä $f(x), g(x) \in K[x]$ ja $g(\alpha) \neq 0$.*

Todistus. On suoraviivaista osoittaa, että osamäärien $f(\alpha)/g(\alpha)$ joukko

$$Q = \{f(\alpha)/g(\alpha) : f(x), g(x) \in K[x], g(\alpha) \neq 0\}$$

muodostaa kunnan. Tämä kunta sisältää kunnan K ja alkion α, joten koska $K(\alpha)$ on määritelmällisesti pienin nämä sisältävä kunta, on oltava $K(\alpha) \subset Q$. □

Lause 2.14. *Olkoon $K(\alpha)$ kunnan K algebrallinen laajennus, ja olkoon $m(x) \in K[x]$ laajennuksen minimipolynomi. Tällöin jokaisella laajennuksen $K(\alpha)$ alkiolla on olemassa yksikäsitteinen esitys $r(\alpha)$, missä $r(x) \in K[x]$ ja $\deg(p(x)) < \deg(m(x))$.*

Todistus. Oletetaan, että $\beta \in K(\alpha)$. Lemman 2.13 nojalla alkio β voidaan esittää muodossa

$$\beta = \frac{f(\alpha)}{g(\alpha)}, \tag{2.15}$$

missä $f(x), g(x) \in K[x]$ ja $g(\alpha) \neq 0$. Koska $g(\alpha) \neq 0$, niin polynomi $g(x)$ ei voi olla jaollinen minimipolynomilla $m(x)$, sillä muutenhan pätisi $g(\alpha) = m(\alpha)q(\alpha) = 0$ jollain

$q(x) \in K[x]$. Toisaalta $m(x)$ on minimipolynomina jaoton, joten se on jaollinen vain itsellään ja vakiopolynomeilla. Koska kuitenkin $g(\alpha) \neq 0$, on oltava $g(x) \neq m(x)$ ja toisaalta jos $g(x)$ olisi vakiopolynomi, se ei puolestaan olisi jaollinen polynomilla $m(x)$. Polynomit $g(x)$ ja $m(x)$ ovat siis keskenään jaottomia.

Polynomien suurin yhteinen tekijä on siis 1, joten Bezout'n lemman nojalla on olemassa sellaiset polynomit $a(x), b(x) \in K[x]$, että

$$a(x)g(x) + b(x)m(x) = 1.$$

Sijoittamalla tähän yhtälöön alkio α nähdään, että

$$a(\alpha)g(\alpha) + b(\alpha)m(\alpha) = a(\alpha)g(\alpha) + b(\alpha) \cdot 0 = a(\alpha)g(\alpha) = 1,$$

joten $g(\alpha) = 1/a(\alpha)$. Sijoittamalla yhtälöön (2.15) saadaan

$$\beta = \frac{f(\alpha)}{g(\alpha)} = f(\alpha)a(\alpha).$$

Merkitään $h(x) = f(x)a(x)$, jolloin $h(x) \in K[x]$.

Soveltamalla polynomien jakoyhtälöä polynomiin $h(x)$ nähdään, että

$$h(x) = q(x)m(x) + r(x)$$

joillakin $q(x), r(x) \in K[x]$, missä $\deg(r(x)) < \deg(m(x))$. Kun näin saatuun yhtälöön sijoitetaan alkio α, saadaan alkiolle β esitys

$$\beta = h(\alpha) = q(\alpha)m(\alpha) + r(\alpha) = r(\alpha),$$

missä $\deg(r(x)) < \deg(m(x))$. (Tapauksessa $r(x) = 0$ asetetaan $\deg(r(x)) = -\infty$.)

Saadun esityksen yksikäsitteisyyden osoittamiseksi oletetaan, että $r_1(\alpha) = r_2(\alpha)$ joillakin $r_1(x), r_2(x) \in K[x]$, missä $\deg(r_1(x)) < \deg(m(x))$ ja $\deg(r_2(x)) < \deg(m(x))$. Tällöin alkio α on erotuspolynomin $s(x) = r_1(x) - r_2(x)$ juuri, sillä $s(\alpha) = r_1(\alpha) - r_2(\alpha) = 0$. Tiedetään kuitenkin, että $\deg(s(x)) < \deg(m(x))$, ja koska alkion α minimipolynomi $m(x)$ on matalinta astetta niistä polynomeista, joiden juuri alkio α on, niin on oltava $s(x) = 0$. Siis $r_1(x) = r_2(x)$. □

Edellisen lauseen nojalla algebrallisen laajennuksen $K(\alpha)$ alkiot ovat siis muotoa

$$k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1},$$

missä n on alkion α minimipolynomin aste ja $k_i \in K$ kaikilla i. Osoittautuukin, että laajennus $K(\alpha)$ on oikeastaan alkion α potenssien α^i virittämä K-vektoriavaruus. Tämä nähdään seuraavassa todistuksessa, jossa näytetään myös, että algebrallisen laajennuksen aste voidaan määrittää suoraan minimipolynomin avulla.

Lause 2.16. *Algebrallisen kuntalaajennuksen $K(\alpha)/K$ aste on yhtä suuri kuin alkion α minimipolynomin aste kunnan K suhteen.*

Todistus. Olkoon $m(x) \in K[x]$ alkion α minimipolynomi kunnan K suhteen, ja oletetaan, että $\deg(m(x)) = n$. Todistetaan väite osoittamalla, että n:n alkion joukko $S = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ on laajennuskunnan $K(\alpha)$ kanta.

Lauseen 2.14 nojalla joukko S virittää laajennuskunnan $K(\alpha)$, sillä jokainen laajennuksen alkio on ilmaistavissa muodossa $r(\alpha) = k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1}$, missä $k_i \in K$ kaikilla i. Esitys on saman lauseen nojalla lisäksi yksikäsitteinen, joten joukko S on laajennuksen $K(\alpha)$ kanta. On siis oltava $[K(\alpha) : K] = n$. □

Esimerkki 2.17. Tarkastellaan laajennusta $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$. Koska $\sqrt{2} \notin \mathbb{Q}$, ei $\sqrt{2}$ voi olla minkään sellaisen polynomin juuri, jonka aste on yksi – muutenhan se olisi jonkin polynomin $h(x) = a_0 + a_1 x \in \mathbb{Q}[x]$ juuri, jolloin $h(\sqrt{2}) = a_0 + a_1\sqrt{2} = 0$, ja edelleen $\sqrt{2} = -a_0/a_1 \in \mathbb{Q}$. Alkion $\sqrt{2}$ minimipolynomin asteen on siis oltava vähintään 2.

Tiedetään, että $\sqrt{2}$ on polynomin $f(x) = x^2 - 2 \in \mathbb{Q}[x]$ juuri. Polynomin $f(x)$ johtokerroin on 1 ja Eisensteinin kriteerin perusteella se on jaoton, joten $f(x)$ on alkion $\sqrt{2}$ minimipolynomi. Näin ollen laajennuksen $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ aste on 2. Lauseen 2.14 nojalla laajennuksen alkiot ovat muotoa $q_0 + q_1\sqrt{2}$, missä $q_0, q_1 \in \mathbb{Q}$.

Edellä on aina mainittu erikseen, että onko yksinkertainen laajennus muotoa $K(\alpha)$ algebrallinen. Käytännön sovelluksissa ei ole kuitenkaan mielekästä aina tarkistaa laajennuksen algebrallisuutta tutkimalla mielivaltaisen laajennuksen alkiota. Onkin hyvä siis ottaa käyttöön muutama laajennuksen virittäjäalkioihin liittyvä tulos, jotka yhdessä antavat tarvitsemamme työvälineet.

Lause 2.18. *Olkoon L kunnan K laajennus. Oletetaan, että jokainen joukon $S \subset L$ alkio on algebrallinen kunnan K suhteen. Tällöin laajennus $K(S)$ on algebrallinen.*

Todistus. Sivuutetaan. Tulos on todistettu esimerkiksi teoksessa [6], s. 11. □

Virittäjäalkioiden ja minimipolynomin avulla saadaan myös yhteys algebrallisten, äärellisten ja äärellisviritteisten laajennusten välille. Seuraava lause osoittaa, että äärellinen laajennus on aina äärellisviritteinen. Äärellisviritteinen laajennus puolestaan on äärellinen vain jos se on myös algebrallinen.

Lause 2.19. *Laajennus L/K on äärellinen, jos ja vain jos L on algebrallinen kunnan K suhteen ja on olemassa äärellinen määrä alkioita $\alpha_1, \alpha_2, \ldots, \alpha_m \in L$, joille pätee $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)$.*

Todistus. Oletetaan, että laajennus L/K on äärellinen astetta n oleva laajennus. Laajennuksella on siis olemassa kanta $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$, joka virittää K-vektoriavaruutena kunnan L, joten on oltava $L \subset K(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Toisaalta $K \subset L$ ja jokainen α_i on kunnan L alkio, joten väistämättä $K(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset L$. Siis $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Osoitetaan vielä, että laajennus L on algebrallinen kunnan K suhteen. Oletetaan, että $\alpha \in L$. Kunnan L dimensio K-vektoriavaruutena on n, joten joukko $\{1, \alpha, \alpha^2, \ldots, \alpha^n\}$ on $n+1$-alkioisena väistämättä lineaarisesti riippuvainen kunnan K suhteen. On siis olemassa nollasta poikkeavat luvut $k_i \in K$, joilla $k_0 + k_1\alpha + \cdots + k_n\alpha^n = 0$. Toisin sanottuna alkio α on siis polynomin $k(x) = k_0 + k_1 x + \cdots + k_n x^n \in K[x]$ juuri ja siten algebrallinen kunnan K suhteen.

Kääntäen, oletetaan, että laajennus $L = K(\alpha_1, \alpha_2, \ldots, \alpha_m)/K$ on algebrallinen. Merkitään $L_i = K(\alpha_1, \ldots, \alpha_i)$, jolloin siis $L_{i+1} = L_i(\alpha_{i+1})$. Käyttämällä nyt induktiota ja lauseita 2.16 ja 2.5 voidaan osoittaa, että laajennus L on äärellinen.

□

Esimerkki 2.20. Laajennus $\mathbb{Q}(\pi)$ on äärellisviritteinen, mutta se ei ole äärellinen, sillä π ei ole algebrallinen kunnan $\mathbb{Q}$ suhteen (tämä on todistettu esimerkiksi teoksessa [8], s. 74).

Luku 3

Laajennusten karakterisointi

Edellisessä luvussa näimme, että rajoittuessamme tarkastelemaan algebrallisia laajennuksia saimme sidottua polynomien teorian kuntalaajennuksiin. Tässä luvussa selvitämme, miten tarkastelua voidaan laajentaa polynomin kaikkiin juuriin osoittamalla, että mille tahansa polynomille on olemassa kerroinkunnan äärellinen laajennus, joka sisältää polynomin kaikki juuret. Määrittelemme itse asiassa niin vaikuttavan juuret sisältävän laajennuksen, että sen tuomia hyötyjä käytetään myöhemmin niin Galois'n teorian peruslauseessa kuin lopulta myös polynomin ratkeavuusehdossa.

Sovellettavuudestaan huolimatta tämä juurikunnaksi kutsuttu laajennus tarvitsee kuitenkin tuekseen tietoja muistakin laajennustyypeistä. Mielekkään informaation saaminen Galois'n teoriassa keskeisistä kuntalaajennusten jonoista vaatii ymmärrystä kunkin välilaajennuksen ominaisuuksista, ja tästä syystä luvun lopuksi käsitellään vielä muutamia tapoja karakterisoida kuntalaajennuksia.

3.1 Juurikunnat

Viidennen asteen polynomilla on korkeintaan viisi juurta, joten kerroinkunnan laajentaminen niistä pelkästään yhdellä ei välttämättä kerro polynomin ratkeavuudesta paljoakaan. Tyypillisesti kuntaa laajennetaankin polynomin kaikilla juurilla, jotta tarkastelu voidaan ulottaa niistä jokaiseen.

Osoitetaan ensin, että minkä tahansa polynomin kaikki juuret voidaan löytää jostain kerroinkunnan äärellisestä laajennuksesta – myös silloin kun polynomin kertoimet eivät ole reaali- tai kompleksilukuja.

Lemma 3.1. *Olkoon $f(x) \in K[x]$ polynomi, jonka aste on n. Tällöin on olemassa kunnan K laajennus M, joka sisältää ainakin yhden polynomin $f(x)$ juurista ja jonka asteelle*

pätee $[M : K] \leq n$. *Lisäksi on olemassa kunnan* K *laajennus* L, *joka sisältää polynomin* $f(x)$ *kaikki juuret ja jonka asteelle pätee* $[L : K] \leq n!$.

Todistus. Osoitetaan ensimmäinen väite rakentamalla kunnan K laajennus, joka sisältää polynomin $f(x)$ juuren. Käytössämme ei kuitenkaan ole soveltuvia välineitä, joilla voitaisiin suoraan rakentaa sopiva laajennus kunnalle K, joten pyritäänkin sen sijaan laajentamaan kunnan K isomorfista kopiota, joka voidaan samaistaa kunnan K kanssa.

Olkoon $p(x) = k_0 + k_1 x + \ldots k_m x^m \in K[x]$ jokin polynomin $f(x)$ jaoton tekijä, jolloin siis $\deg(p(x)) = m \leq n$. Määritellään kuvaus

$$\phi\colon K \to K[x]/\langle p(x)\rangle, \quad \phi(k) = k + \langle p(x)\rangle,$$

joka siis kuvaa kunkin kunnan K alkion omalle sivuluokalleen.

Osoitetaan, että rajoittumakuvaus $\phi\colon K \to \phi(K)$ on isomorfismi. Polynomi $p(x)$ on jaoton, joten sen ideaali $\langle p(x)\rangle = \{q(x)p(x) : q(x) \in K[x]\}$ on maksimaalinen, mistä seuraa, että tekijärakenne $K[x]/\langle p(x)\rangle$ on kunta. Kuvaus ϕ on homomorfismi, ja koska kuntien väliset homomorfismit ovat tunnetusti aina injektiivisiä, niin myös kuvaus ϕ on injektio. Rajoittumakuvauksen määritelmästä seuraa suoraan, että ϕ on myös surjektio, joten kuvaus ϕ isomorfismi.

Merkitään $M = K[x]/\langle p(x)\rangle$. Kunta K on siis isomorfinen kunnan M alikunnan $\phi(K)$ kanssa, joten kunta M voidaan tulkita kunnan K laajennuksena. Laajennuskunta M koostuu K-kertoimisten polynomien edustamista sivuluokista, joten tässä tulkinnassa kunta K on puolestaan vakiopolynomien edustamien sivuluokkien joukko $\{k + \langle p(x)\rangle\}$.

Samaistetaan kunta K nyt isomorfisen kuvansa kanssa. Tällöin polynomi $p(x)$ saa muodon

$$p(x) = (k_0 + \langle p(x)\rangle) + (k_1 + \langle p(x)\rangle)x + \cdots + (k_m + \langle p(x)\rangle)x^m.$$

Olkoon $\alpha = x + \langle p(x)\rangle \in M$. Osoitetaan, että sivuluokka α on polynomin $p(x)$ juuri. On siis osoitettava, että

$$p(x + \langle p(x)\rangle) = \langle p(x)\rangle.$$

Nyt

$$\begin{aligned}
&p(x + \langle p(x)\rangle)\\
&= (k_0 + \langle p(x)\rangle) + (k_1 + \langle p(x)\rangle)(x + \langle p(x)\rangle) + \cdots + (k_m + \langle p(x)\rangle)(x + \langle p(x)\rangle)^m\\
&= (k_0 + \langle p(x)\rangle) + (k_1 x + \langle p(x)\rangle) + \cdots + (k_m x^m + \langle p(x)\rangle)\\
&= p(x) + \langle p(x)\rangle\\
&= \langle p(x)\rangle,
\end{aligned}$$

joten väite pätee. Polynomi $p(x)$ on kuitenkin polynomin $f(x)$ tekijä, joten alkio α on myös polynomin $f(x)$ juuri. Polynomilla $f(x)$ on siis juuri α laajennuksessa M.

Osoitetaan vielä, että $[M : K] \leq n$. Olkoon $h(x) + \langle p(x) \rangle$ mielivaltainen laajennuskunnan M alkio. Tällöin polynomien jakoyhtälöstä saadaan

$$h(x) = q(x)p(x) + r(x) = r(x) + q(x)p(x),$$

missä $\deg(r(x)) \leq \deg(p(x)) = m$. Näin saadusta esityksestä polynomille $h(x)$ kuitenkin nähdään suoraan, että

$$h(x) \in r(x) + \langle p(x) \rangle,$$

joten

$$h(x) + \langle p(x) \rangle = r(x) + \langle p(x) \rangle.$$

Mielivaltainen kunnan M alkio voidaan siis esittää muodossa

$$\begin{aligned} &r_0 + r_1 x + \cdots + r_{m-1} x^{m-1} + \langle p(x) \rangle \\ &= (r_0 + \langle p(x) \rangle) + (r_1 + \langle p(x) \rangle)(x + \langle p(x) \rangle) + \cdots + (r_{m-1} + \langle p(x) \rangle)(x^{m-1} + \langle p(x) \rangle), \end{aligned}$$

joten sivuluokat

$$1 + \langle p(x) \rangle, \;\; x + \langle p(x) \rangle, \;\; \ldots \;\; , \;\; x^{m-1} + \langle p(x) \rangle$$

muodostavat siis laajennuksen M/K kannan. Näin ollen $[M : K] = m \leq n$.

Osoitetaan lauseen toinen osa käyttämällä induktiota polynomin $f(x)$ asteen suhteen. Tapauksessa $\deg(f(x)) = 1$ väite pätee suoraan, sillä kunta K on itsensä laajennus, ja polynomi $f(x)$ on puolestaan muotoa $a_0 + a_1 x$, jolloin sillä on siis juuri $-a_0/a_1 \in K$. Laajennuksen K kanta on $\{1\}$, joten lisäksi $[K : K] = 1$.

Oletetaan nyt, että väite pätee jollain $k \in \mathbb{N}$. Olkoon $\deg(f(x)) = k + 1$. Lauseen ensimmäisen osan perusteella on olemassa laajennus M/K, jossa polynomilla $f(x)$ on juuri α ja jolle pätee $[M : K] \leq k + 1$. Tällöin siis

$$f(x) = (x - \alpha)g(x)$$

jollain $g(x) \in M[x]$, missä $\deg(g(x)) = k$. Soveltamalla induktio-oletusta polynomiin $g(x)$ saadaan siis kunnan M laajennus L, missä polynomi $g(x)$ jakautuu ensimmäisen asteen tekijöihin ja jolle pätee $[L : M] \leq k!$. Mutta nyt myös $f(x)$ jakautuu ensimmäisen asteen termien tuloksi laajennuksessa L, joten laajennus L sisältää siis polynomin $f(x)$ kaikki juuret. Lisäksi lausetta 2.5 soveltamalla saadaan

$$[L : K] = [L : M][M : K] \leq k! \cdot (k + 1) = (k + 1)!,$$

mikä oli osoitettava. □

Siinä missä kerroinkunnan laajentaminen vain joillakin polynomin juurista ei anna polynomista tarpeeksi tietoa, kunnan laajentaminen varomattomasti saattaa johtaa epäkäytännöllisen suureen laajennuskuntaan. Esimerkissä 2.17 kerroinkunta $\mathbb{Q}$ olisi voitu laajentaa suoraan kaikki juuret sisältäväksi kunnaksi $\mathbb{C}$, mutta silloin emme olisi saaneet yksityiskohtaista tietoa pienemmästä laajennuksesta $\mathbb{Q}(\sqrt{2})$ ja sen alkioista – ja Galois'n teoria perustuu nimenomaan tarkasti määriteltyjen kuntalaajennusten jonoihin.

Onkin siis syytä pyrkiä tarkastelemaan pienintä kerroinkunnan laajennusta, joka sisältää polynomin kaikki juuret. Tällaista laajennusta kutsutaan polynomin *juurikunnaksi*.

Määritelmä 3.2. Olkoon $p(x) \in K[x]$. Kunnan K laajennus L on polynomin $p(x)$ *juurikunta* kunnan K suhteen, jos

1. Polynomi $p(x)$ jakautuu renkaassa $L[x]$ ensimmäisen asteen polynomien tuloksi, ja
2. $L = K(\alpha_1, \ldots, \alpha_n)$, missä $\alpha_1, \ldots, \alpha_n \in L$ ovat polynomin $p(x)$ juuret.

Laajennus L on polynomijoukon $S \subset K[x]$ juurikunta, jos jokainen polynomi $p(x) \in S$ jakautuu ensimmäisen asteen polynomien tuloksi renkaassa $L[x]$ ja lisäksi $L = K(A)$, missä A on joukon S polynomien kaikkien juurten joukko.

Polynomin kaikkien juurten löytyminen on juurikunnan käsitteen ydinajatus, mutta määritelmässä 3.2 se ilmaistaan yhtäpitävällä tavalla vaatimalla, että polynomi jakautuu juurikunnassa ensimmäisen asteen termien tuloksi. Tätä ominaisuutta hyödynnetään monissa myöhemmissä todistuksissa, ja se onkin niin keskeinen, että englanniksi juurikunta onkin *splitting field* eli kunta, jossa polynomi "jakautuu".

Määritelmän 3.2 ehto 2 puolestaan varmistaa, että juurikunta on nimenomaan pienin polynomin juuret sisältävä laajennus. Lauseen 2.18 nojalla ehdosta 2 seuraa myös, että juurikunta on aina algebrallinen laajennus. Näin ollen juurikunta on aina myös äärellinen lauseen 2.19 nojalla.

Lemman 3.1 avulla voidaan todistaa, että juurikunta on aina olemassa. Samalla polynomilla voi kuitenkin olla monta erilaiselta vaikuttavaa juurikuntaa riippuen siitä, miten polynomin kerroinkunta on valittu, mutta myöhemmin osoitetaan, että polynomin juurikunnat ovat isomorfisia kerroinkunnan valinnasta riippumatta.

Korollaari 3.3. *Jokaisella polynomilla $f(x) \in K[x]$ on juurikunta kunnan K suhteen.*

Todistus. Olkoon $f(x) \in K[x]$. Lemman 3.1 nojalla on olemassa laajennus L/K, jossa $f(x)$ jakautuu ensimmäisen asteen tekijöihin. Jos $\alpha_1, \ldots, \alpha_n \in L$ ovat polynomin $f(x)$ juuret, niin $K(\alpha_1, \ldots, \alpha_n) \subset L$ on tällöin polynomin $f(x)$ juurikunta. □

Olkoon $K(\alpha_1, \ldots, \alpha_n)$ polynomin $f(x) \in K[x]$ juurikunta. Näytetään seuraavaksi, että juurikunnan alkiot ovat ilmaistavissa K-lineaarikombinaatioina juurien α_i potensseista.

Algebrallisen laajennuksen $K(\alpha_1)$ alkiot ovat lauseen 2.14 nojalla muotoa $\sum_i k_i \alpha_1^i$, missä $k_i \in K$ kaikilla i. Vastaavasti laajennuksen $K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2)$ alkiot ovat muotoa $\sum_j l_j \alpha_2^j$, missä $l_j \in K(\alpha_1)$ kaikilla j. Näin ollen laajennuksen $K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2)$ alkiot ovat muotoa

$$\begin{aligned} \sum_j l_j \alpha_2^j &= \sum_j \Big(\sum_i k_i \alpha_1^i \Big) \alpha_2^j \\ &= \sum_j \sum_i k_{ij} \alpha_1^i \alpha_2^j \end{aligned} \tag{3.4}$$

missä $k_{ij} \in K$. Jatkamalla vastaavasti muille juurille nähdään, että itse juurikunnan $K(\alpha_1, \ldots, \alpha_n)$ alkiot ovat muotoa

$$\sum_{i_n} \sum_{i_{n-1}} \cdots \sum_{i_1} k_i \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}, \tag{3.5}$$

missä $i = (i_1, \ldots, i_n)$.

Yllä olevista esityksistä (3.4) on usein havainnollisempi, mutta (3.5) on hyödyllinen myöhemmissä todistuksissa. Erityisesti on huomattava, että mikä tahansa juurikunnan alkio voidaan esittää muodossa, jossa on vain kertoimia k kunnasta K ja alkioita α_i.

Esimerkki 3.6. Olkoon $f(x) = x^4 - 5x + 6 = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$. Polynomin ainoat juuret ovat $\pm\sqrt{2}$ ja $\pm\sqrt{3}$, joten polynomin juurikunta on $\mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$. Algebrallinen laajennus $\mathbb{Q}(\sqrt{2})$ kuitenkin sisältää jo alkion $-\sqrt{2} = -1 \cdot \sqrt{2}$, joten sitä ei ole tarpeen lisätä enää erikseen.

Lisätään laajennukseen $\mathbb{Q}(\sqrt{2})$ vielä alkio $\sqrt{3}$. Laajennuksen $\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ alkiot ovat tuloksen (3.4) perusteella muotoa

$$(q_0 + q_1\sqrt{2}) + (r_0 + r_1\sqrt{2})\sqrt{3} \tag{3.7}$$

joillakin $q_i, r_i \in \mathbb{Q}$. Nyt kuitenkin jälleen pätee $-\sqrt{3} = -1 \cdot \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, joten polynomin $f(x)$ juurikunta on $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, ja sen alkiot ovat yhtälössä (3.7) esitettyä muotoa.

3.2 Normaalit ja separoituvat laajennukset

Polynomin juurikunnalta vaaditaan, että polynomi jakautuu juurikunnassa ensimmäisen asteen tekijöihin, minkä tarkistaminen voi olla vaivalloista varsinkin, jos polynomin juurten lukumäärä on suuri. Tehtävä kuitenkin helpottuu, jos yhden juuren löytyminen laajennuskunnasta takaa kaikkien juurten löytymisen. Tällöin puhutaan normaalista laajennuksesta.

Määritelmä 3.8. Laajennus L/K on *normaali*, jos jokainen kunnan K jaoton polynomi, jolla on ainakin yksi juuri kunnassa L, jakautuu ensimmäisen asteen tekijöiksi kunnassa L.

Viidennen asteen polynomilla on korkeintaan viisi juurta, mutta mikään ei kuitenkaan takaa etteivätkö jotkin niistä voisi olla samoja. Tällainen *moninkertaisten juurten* tapaus olisi ongelmallinen, sillä tavoitteenamme on laajentaa tarkasteltavan polynomin kerroinkuntaa yksittäinen juuri kerrallaan. Moninkertaiset juuret eivät tuo laajennuksiin lisäinformaatiota, sillä vain erilliset juuret tuottavat erillisiä kerroinkunnan laajennuksia. Tämän tilanteen välttämiseksi otetaan käyttöön separoituvuuden käsite niin polynomien kuin laajennustenkin suhteen.

Määritelmä 3.9. Olkoon L polynomin $f(x) \in K[x]$ juurikunta. Alkio $\alpha \in L$ on polynomin $f(x)$ *moninkertainen juuri*, jos $f(x)$ on jaollinen polynomilla $(x-\alpha)^k$ jollain $k > 1$. Jos polynomilla $f(x)$ ei ole moninkertaisia juuria, sen sanotaan olevan *separoituva*.

Määritelmä 3.10. Laajennuksen L/K alkio $a \in L$ on *separoituva*, jos sen minimipolynomi kunnan K suhteen on separoituva. Koko laajennus puolestaan on separoituva, jos sen jokainen alkio on separoituva.

Toisin sanottuna moninkertaisten juurten olemassaolo tekisi polynomiyhtälön ratkaisemisesta helpompaa, mutta sitä emme halua, sillä lopullisena tavoitteenamme on löytää jokin niin hankala viidennen asteen polynomiyhtälö, ettei se ratkea juurtamalla. Seuraava lause antaakin avuksemme ehdon polynomin separoituvuudelle.

Lause 3.11. *Jos kunnan K karakteristika on 0, kaikki jaottomat K-kertoimiset polynomit ovat separoituvia.*

Todistus. Oletetaan, että K on kunta, jonka karakteristika on 0. Olkoon $f(x) = k_0 + k_1 x + \cdots + k_n x^n \in K[x]$ jaoton polynomi, jonka johtokertoimelle k_n pätee $k_n \neq 0$. Määritellään polynomin $f(x)$ derivaatta $f'(x) = k_1 + 2k_2 x + \cdots + nk_n x^{n-1}$. Polynomeille pätevät tutut derivointisäännöt: esimerkiksi teokset [8] ja [9] käsittelevät aihetta tarkemmin.

Olkoon L polynomin $f(x) \in K[x]$ juurikunta. Oletetaan, että polynomi $f(x)$ ei ole separoituva, jolloin sillä on moninkertainen juuri $\alpha \in L$. Polynomi $f(x)$ voidaan siis esittää muodossa $f(x) = (x-\alpha)^2 g(x)$, joten

$$f'(x) = 2(x-\alpha)g(x) + (x-\alpha)^2 g'(x) = (x-\alpha)(2g(x) + (x-\alpha)g'(x)).$$

Nähdään, että alkio α on siis myös polynomin $f'(x)$ juuri.

Olkoon $m(x)$ alkion α minimipolynomi kunnassa K. Alkio α on sekä polynomin $f(x)$ että polynomin $f'(x)$ juuri, joten ne ovat lauseen 2.12 mukaan molemmat jaollisia polynomilla $m(x)$. Oletuksen nojalla $f(x)$ on kuitenkin jaoton, joten polynomien $m(x)$ ja $f(x)$ on

oltava samaa astetta. Derivaatta $f'(x)$ on näistä kuitenkin alempaa astetta, mutta koska $m(x)$ kuitenkin jakaa sen, on välttämättä oltava $f'(x) = 0$.

Näin ollen derivaatan $f'(x)$ johtokertoimelle nk_n pätee $nk_n = 0$, mutta kunnan K karakteristika on 0, joten on oltava $k_n = 0$. Tämä on kuitenkin mahdotonta, sillä k_n on polynomin $f(x)$ korkeimman asteen termin kerroin eikä siten voi olla 0. □

Moninkertaisten juurien välttämiseksi joissakin Galois'n teoriaan liittyvissä teoksissa oletetaan kerroinkunnan karakteristikan olevan aina nolla. Tässä esityksessä tätä oletusta ei kuitenkaan tehdä, vaan separoituvuus mainitaan aina tarvittaessa.

Esimerkki 3.12. Kunnan $\mathbb{Q}$ karakteristika on nolla, sillä $n \cdot 1 \neq 0$ millä tahansa n. Tästä seuraa, että kaikki jaottomat $\mathbb{Q}$-kertoimiset polynomit ovat separoituvia, joten myös esimerkissä 3.6 käsitelty juurikunta $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ on separoituva. Myöhemmin osoitetaan, että separoituvan polynomin juurikunta on aina myös normaali.

Luku 4

Kuntien väliset kuvaukset

Monissa käytännön tilanteissa on tarpeen tarkastella polynomin kerroinkunnan isomorfisia kopioita, joten on syytä tutkia, miten eri kerroinkunnista muodostetut juurikunnat suhtautuvat toisiinsa. Tässä luvussa osoitetaankin, että juurikunnan käsite on niin yleismaailmallinen, että juurikunta on polynomin kerroinkunnan kopion valinnasta riippumatta yksikäsitteinen – isomorfiaa vaille. Tämä todistetaan varsin taloudellisesti *jatkamalla* olemassa olevia kuntaisomorfismeja uusien konstruoimisen sijaan.

Tämä isomorfismeihin keskittyvä lähestymistapa on enne tulevasta, sillä luvun keskeisintä tulosta käytetään myöhemmin rakentamaan kuvauksia, jotka permutoivat polynomin juuria. Yhdessä nämä kuvaukset muodostavat juurten symmetriaryhmiä, joiden varaan Galois perusti ratkeavuuden teoriansa.

4.1 Isomorfismien jatkaminen

Osoitetaan ensin, että isomorfisten kuntien samaa astetta olevat yksinkertaiset algebralliset laajennukset ovat isomorfisia. Tulos voidaan itse asiassa laajentaa koskemaan muitakin kuin yksinkertaisia algebrallisia laajennuksia, sillä mikä tahansa algebrallinen laajennus muotoa $K(\alpha_1, \ldots, \alpha_n)$ voidaan ilmaista yksinkertaisena algebrallisena laajennuksena (mikä on todistettu esimerkiksi teoksessa [7], s. 312).

Lause 4.1. *Olkoon $\sigma\colon K \to K'$ kuntaisomorfismi. Olkoon α jaottoman polynomin $p(x) \in K[x]$ juuri ja α' polynomin $\sigma(p(x))$ juuri. Tällöin on olemassa kuvausta σ jatkava isomorfismi $\phi\colon K(\alpha) \to K'(\alpha')$, jolla $\phi(\alpha) = \alpha'$ ja $\phi|_K = \sigma$.*

Todistus. Olkoon $m(x) \in K[x]$ alkion α minimipolynomi. Lauseen 2.14 nojalla mikä tahansa alkio $a \in K(\alpha)$ on ilmaistavissa yksikäsitteisessä muodossa $a = k_0 + k_1\alpha + \cdots + k_n\alpha^n$,

missä $k_i \in K$ ja $n = \deg(m(x)) - 1$. Osoitetaan, että kuvaus

$$\phi\colon K(\alpha) \to K'(\alpha'), \qquad \phi(a) = \sigma(k_0) + \sigma(k_1)\alpha' + \cdots + \sigma(k_n)(\alpha')^n$$

on etsimämme kuvaus.

Osoitetaan ensin, että ϕ on isomorfismi. On suoraviivaista osoittaa, että kaikilla $a, b \in K(\alpha)$ pätee $\phi(a+b) = \phi(a) + \phi(b)$, joten osoitetaan vielä, että $\phi(ab) = \phi(a)\phi(b)$. Olkoot $a, b \in K(\alpha)$. Lauseen 2.14 perusteella alkiot a, b ja ab voidaan esittää muodossa $a = f(\alpha)$, $b = g(\alpha)$ ja $ab = h(\alpha)$ joillakin polynomeilla $f(x), g(x), h(x) \in K[x]$, joista kunkin aste on pienempi kuin $\deg(m(x))$. Nyt

$$f(\alpha)g(\alpha) - h(\alpha) = ab - ab = 0,$$

joten alkio α on polynomin $f(x)g(x) - h(x) \in K[x]$ juuri ja siksi lauseen 2.12 nojalla alkion α minimipolynomi $m(x)$ jakaa sen. On siis olemassa sellainen polynomi $q(x) \in K[x]$, että $f(x)g(x) - h(x) = m(x)q(x)$, joten

$$f(x)g(x) = m(x)q(x) + h(x). \tag{4.2}$$

Polynomi $p(x)$ oletettiin jaottomaksi, ja kuitenkin lauseen 2.12 perusteella polynomi $m(x)$ jakaa sen, joten polynomien $p(x)$ ja $m(x)$ on oltava samaa astetta. On siis oltava $p(x) = km(x)$ jollain vakiolla $k \in K$. Kuvaus σ oletettiin kuitenkin kuntahomomorfismiksi, joten oletuksesta $\sigma(p(\alpha')) = 0$ seuraa $p(\alpha') = 0$, sillä kuntahomomorfismi on aina myös injektio. Näin ollen $p(\alpha') = km(\alpha') = 0$, mistä seuraa, että $m(\alpha') = 0$. Sijoittamalla alkio α' yhtälöön (4.2) saadaan siis

$$f(\alpha')g(\alpha') = m(\alpha')q(\alpha') + h(\alpha') = 0 \cdot q(\alpha') + h(\alpha') = h(\alpha'). \tag{4.3}$$

Yhtälöä 4.3 soveltamalla saadaan

$$\phi(ab) = \phi(h(\alpha)) = \sigma(h(\alpha')) = \sigma(f(\alpha')g(\alpha')),$$

missä $\sigma(f(\alpha')g(\alpha'))$ on polynomin $f(x)g(x)$ kuva $\sigma(f(x)g(x))$, johon on sijoitettu alkio α'. Kuvauksen σ indusoima kuvaus $\sigma\colon K[x] \to K'[x]$ on kuitenkin isomorfismi (aihetta käsitellään tarkemmin esimerkiksi teoksessa [11], s. 369), joten lopulta

$$\sigma(f(\alpha')g(\alpha')) = \sigma(f(\alpha'))\sigma(g(\alpha')) = \phi(f(\alpha))\phi(g(\alpha)) = \phi(a)\phi(b).$$

Kuvaus ϕ on siis kuntien välinen homorfismi, jolloin se on tunnetusti myös injektio. Osoitetaan vielä, että ϕ on surjektio. Olkoon $b \in K'(\alpha')$, jolloin lauseen 2.14 nojalla

$b = k_0' + k_1'\alpha' + \cdots + k_n'(\alpha')^n$ joillakin $k_i' \in K'$. Kuvaus σ on isomorfismina kuitenkin bijektio, joten kaikilla $k_i' \in K'$ on olemassa jokin $k_i \in K$, jolla $\sigma(k_i) = k_i'$. Nyt siis

$$\begin{aligned} b = k_0' + k_1'\alpha' + \cdots + k_n'(\alpha')^n &= \sigma(k_0) + \sigma(k_1)\alpha' + \cdots + \sigma(k_n)(\alpha')^n \\ &= \phi(k_0 + k_1\alpha + \cdots + k_n\alpha^n), \end{aligned}$$

missä $k_0 + k_1\alpha + \cdots + k_n\alpha^n \in K(\alpha)$, joten ϕ on surjektio.

Kuvaus $\phi\colon K(\alpha) \to K'(\alpha')$ on siis isomorfismi, joten laajennukset $K(\alpha)$ ja $K'(\alpha')$ ovat isomorfiset. Lisäksi kuvauksen ϕ määritelmästä seuraa suoraan, että $\phi(\alpha) = \alpha'$ ja millä tahansa $k \in K$ pätee $\phi(k) = \sigma(k)$. □

Isomorfismien jatkamisen täsmällinen käsittely vaatii Zornin lemman käyttämistä. Määritellään tätä varten Zornin lemman käyttämä kaksipaikkaisten relaatioiden terminologia.

Määritelmä 4.4. Olkoon $\mathcal{P}$ joukko ja $\leq$ sen kaksipaikkainen relaatio. Tarkastellaan seuraavia ehtoja:

1. Kaikilla $a \in \mathcal{P}$ pätee $a \leq a$.
2. Jos $a \leq b$ ja $b \leq c$, niin $a \leq c$.
3. Jos $a \leq b$ ja $b \leq a$, niin $a = b$.
4. Kaikilla $a, b \in \mathcal{P}$ pätee $a \leq b$ tai $b \leq a$.

Jos ehdot 1-3 pätevät, paria $(\mathcal{P}, \leq)$ kutsutaan *osittaisjärjestykseksi*. Parin sanotaan olevan *lineaarijärjestys* tai *täydellinen järjestys*, jos myös neljäs ehto pätee. Jos jokin osittaisjärjestyksen osajoukko on lineaarijärjestys, sen sanotaan olevan *ketju*. Alkio $m \in \mathcal{P}$ on osajoukon $A \subset \mathcal{P}$ *yläraja*, jos $a \leq m$ kaikilla $a \in A$. Alkio m on *maksimaalinen*, jos millään alkiolla $a \in \mathcal{P}$ ei päde $m \leq a$ ja $a \neq m$.

Lemma 4.5. (Zornin lemma.) *Olkoon $\mathcal{P}$ epätyhjä osittaisjärjestys, jonka jokaisella ketjulla on yläraja. Tällöin $\mathcal{P}$ sisältää maksimaalisen alkion.*

Todistus. Sivuutetaan. Tulos on todistettu esimerkiksi teoksessa [11], s. 776. □

Zornin lemma apunamme olemme valmiit käsittelemään kahden kunnan välisen isomorfismin jatkamista juurikuntien väliseksi isomorfismiksi. Isomorfismien jatkamiselle esitellään tärkeä sovellus jo tämän luvun lopussa, mutta oikeuksiinsa se pääsee kunnolla vasta myöhemmin. Identtinen kuvaus $\mathrm{id}\colon K \to K$ on nimittäin myös kuntaisomorfismi, joten lauseen 4.6 avulla voidaan määritellä sellaisia isomorfismeja, jotka kiinnittävät lähtökunnan K ja siten liikuttavat vain alkioita, jotka ovat laajennuskunnassa L, kuten esimerkiksi

polynomin juuria. Myöhemmin osoitetaankin, että tällaiset isomorfismit kuvaavat polynomin juuret toisilleen, ja niistä voidaan jopa muodostaa juurten permutaatioryhmiä – niin sanottuja *Galois'n ryhmiä*.

Lause 4.6. (Isomorfismien jatkaminen.) *Olkoon $\sigma\colon K \to K'$ kuntaisomorfismi, ja olkoot $S \subset K[x]$ ja vastaavasti $S' = \{\sigma(f(x)) \in K'[x] : f(x) \in S\}$ polynomijoukkoja. Olkoon L joukon S juurikunta kunnan K suhteen ja L' vastaavasti joukon S' juurikunta kunnan K' suhteen. Tällöin on olemassa isomorfismi $\tau\colon L \to L'$, jolla $\tau|_K = \sigma$.*

Olkoon $\alpha \in L$ jaottoman polynomin $f(x) \in K[x]$ juuri. Jos $\alpha' \in L'$ on polynomin $\sigma(f(x))$ juuri, niin kuvaus τ voidaan valita sellaiseksi, että $\tau(\alpha) = \alpha'$.

Todistus. Osoitetaan ensin lauseen ensimmäinen osa. Olkoon $\mathcal{I}$ kaikkien sellaisten parien (I, γ) joukko, jossa I on kunnan L alikunta ja $\gamma\colon I \to L'$ on sellainen kuntahomomorfismi, että $\gamma|_K = \sigma$. Joukko $\mathcal{I}$ on epätyhjä, sillä siinä on ainakin pari (K, σ). Parin $(\mathcal{I}, \leq)$ voidaan osoittaa olevan osittaisjärjestys, kun määritellään relaatio $\leq$ seuraavasti:

$$(I, \gamma) \leq (I', \gamma'), \text{ jos } I \subset I' \text{ ja } \gamma'|_I = \gamma.$$

Olkoon $\{(I_j, \gamma_j)\}$ nyt jokin ketju osittaisjärjestyksessä $(\mathcal{I}, \leq)$. Määritellään kuvaus $\bar{\gamma}\colon \cup_j I_j \to L'$ asettamalla $\bar{\gamma}(a) = \gamma_j(a)$, kun $a \in I_j$. Nyt pari $(\cup_j I_j, \bar{\gamma}) \in \mathcal{I}$ on ketjun $\{(I_j, \gamma_j)\}$ yläraja. Zornin lemman mukaan osittaisjärjestyksessä $(\mathcal{I}, \leq)$ on siis olemassa maksimaalinen alkio (M, τ). Osoitetaan, että kuvaus τ on etsitty isomorfismi näyttämällä, että $M = L$ ja $M' = L'$, kun merkitään $M' = \tau(M)$.

Osoitetaan ensin, että $M = L$. Joukon $\mathcal{I}$ määritelmästä seuraa, että $M \subset L$, joten riittää osoittaa, että $L \subset M$. Oletetaan, että $L \not\subset M$. Juurikunta L on pienin kunta, joka sisältää joukon S polynomien juuret, joten on siis olemassa jokin polynomi $f(x) \in S$, jonka kaikki juuret eivät ole kunnassa M. Olkoon $\delta \in L \setminus M$ tällainen polynomin $f(x)$ juuri ja $m_\delta(x) \in K[x] \subset M[x]$ sen minimipolynomi kunnan K suhteen. Minimipolynomi $m_\delta(x)$ jakaa lauseen 2.12 perusteella polynomin $f(x)$, joten homomorfismin laskusääntöjä soveltamalla nähdään, että polynomi $\sigma(m_\delta(x)) \in K'[x] \subset M'[x]$ jakaa puolestaan polynomin $\sigma(f(x))$.

Polynomi $\sigma(f(x))$ jakautuu kuitenkin ensimmäisen asteen termien tuloksi juurikunnassa L' ja polynomi $\sigma(m_\delta(x))$ jakaa sen, joten polynomilla $\sigma(m_\delta(x))$ on oltava jokin juuri $\delta' \in L'$. Alkio δ on siis jaottoman M-kertoimisen polynomin $m_\delta(x)$ juuri ja δ' on jaottoman M'-kertoimisen polynomin $\sigma(m_\delta(x))$ juuri, joten lauseen 4.1 nojalla on olemassa kuvausta τ jatkava isomorfismi $\phi\colon M(\delta) \to M'(\delta') \subset L'$, jolla $\phi|_M = \tau$.

Nyt kuitenkin $(M, \tau) \leq (M(\delta), \phi)$, sillä $M \subset M(\delta)$ ja $\phi|_M = \tau$, mikä on ristiriita, sillä pari (M, τ) on maksimaalinen. On siis oltava $M = L$.

Osoitetaan vielä, että $M' = L'$. Joukon $\mathcal{I}$ määritelmästä seuraa, että $M' \subset L'$, joten riittää osoittaa, että $L' \subset M'$. Osoitetaan, että joukon S' polynomit jakautuvat ensimmäisen asteen termien tuloksi kunnassa M'. Olkoon $f_i(x) \in S$. Koska kunta L on joukon

S juurikunta, niin polynomi $f_i(x)$ voidaan ilmaista muodossa $f_i(x) = k\prod_j(x-\alpha_j)$, missä alkiot $\alpha_j \in L$ ovat polynomin $f_i(x)$ juuret ja $k \in K$. Näin siis

$$\tau(f_i(x)) = \tau(k)\prod_j(x-\tau(\alpha_j)),$$

ja kukin $\tau(f_i(x))$ siis jakautuu ensimmäisen asteen termien tuloksi kunnassa M'. Juurikunta L' on kuitenkin määritelmällisesti pienin kunta, jossa näin tapahtuu, joten on oltava $L' \subset M'$ ja edelleen $M' = L'$. Näin ollen $\tau\colon L \to L'$, ja joukon $\mathcal{I}$ määritelmästä seuraa, että $\tau|_K = \sigma$, mikä oli osoitettava.

Osoitetaan vielä lauseen toinen osa. Polynomi $f(x) \in K[x]$ on jaoton, joten myös polynomi $\sigma(f(x)) \in K'[x]$ on jaoton. Näin ollen lauseen 4.1 nojalla on olemassa isomorfismi $\rho\colon K(\alpha) \to K'(\alpha')$, jolla $\rho(\alpha) = \alpha'$. Nyt voidaan soveltaa aiempaa päättelyä kuvaukseen ρ, ja jatkaa se sellaiseksi isomorfismiksi $\tau\colon L \to L'$, että $\tau|_{K(\alpha)} = \rho$. Lisäksi tiedetään, että $\alpha \in K(\alpha)$, joten $\tau(\alpha) = \rho(\alpha) = \alpha'$.

□

4.2 Juurikuntiin liittyviä tuloksia

Isomorfismien jatkamislauseesta seuraa välittömästi, että polynomijoukon – ja siten myös yksittäisen polynomin – juurikunta on isomorfiaa vaille yksikäsitteinen. Pian käsiteltävä esimerkki 4.8 tutkii aihetta tarkemmin.

Korollaari 4.7. *Olkoon K kunta ja $S \subset K[x]$. Tällöin kaikki polynomijoukon S juurikunnat kunnan K suhteen ovat isomorfisia kunnan K laajennuksina.*

Todistus. Identtinen kuvaus $K \to K$ on kuntaisomorfismi, joten lauseen 4.6 nojalla se voidaan jatkaa kunnan K laajennusten isomorfismiksi kahden minkä tahansa joukon S juurikunnan välille. □

Todistuksessa sovellettiin isomorfismin jatkamislausetta identtiseen kuvaukseen, mutta mikään ei estä tekemästä samaa kahden mielivaltaisen kunnan väliselle isomorfismille. Näin voidaankin osoittaa, että polynomin juurikunnat keskenään isomorfisten kerroinkuntien suhteen ovat isomorfisia. Tätä tietoa hyödynnetään pian lauseen 4.9 todistuksessa.

Esimerkki 4.8. Tarkastellaan laajennusta $\mathbb{Q}(\sqrt{2})$. Esimerkissä 2.17 osoitettiin, että laajennuksen minimipolynomi on $x^2 - 2 \in \mathbb{Q}[x]$. Laajennus $\mathbb{Q}(\sqrt{2})$ on kuitenkin pienin niistä kunnan $\mathbb{Q}$ laajennuksista, jotka sisältävät polynomin $x^2 - 2$ molemmat juuret $\pm\sqrt{2}$, joten se on itse asiassa polynomin $x^2 - 2$ juurikunta. Etsitään polynomille nyt toinenkin juurikunta, ja tarkastellaan, miltä sen alkiot näyttävät.

Määritellään kuvaus

$$\phi\colon \mathbb{Q} \to \mathbb{Q}[x]/\langle x^2-2\rangle, \quad \phi(q) = q + \langle x^2-2\rangle.$$

Lemman 3.1 todistuksessa näytettiin, että kuvauksen ϕ lähtöjoukko $\mathbb{Q}$ on isomorfinen maalijoukon

$$K' = \{q + \langle x^2-2\rangle : q \in \mathbb{Q}\}$$

kanssa, joten kunta $\mathbb{Q}$ voidaan samaistaa tämän joukon kanssa, ja kunta $\mathbb{Q}[x]/\langle x^2-2\rangle$ on siten kunnan $\mathbb{Q}$ laajennus. Samaisessa todistuksessa 3.1 näytettiin myös, että sivuluokka

$$\alpha = x + \langle x^2-2\rangle \in \mathbb{Q}[x]/\langle x^2-2\rangle$$

on polynomin x^2-2 juuri. Vastaavasti nähdään, että myös sivuluokka $-\alpha = -x+\langle x^2-2\rangle$ on polynomin x^2-2 juuri, sillä

$$(-x + \langle x^2-2\rangle)^2 + (-2 + \langle x^2-2\rangle) = (x^2-2) + \langle x^2-2\rangle = \langle x^2-2\rangle.$$

Polynomin x^2-2 molemmat juuret ovat siis α ja $-\alpha$, joten sen juurikunta kunnan K' suhteen on $K'(\alpha)$.

Osoitetaan vielä, että $K'(\alpha) = \mathbb{Q}[x]/\langle x^2-2\rangle$. Juurikunta $K'(\alpha)$ sisältyy laajennukseen $\mathbb{Q}[x]/\langle x^2-2\rangle$, joten riittää osoittaa, että $\mathbb{Q}[x]/\langle x^2-2\rangle \subset K'(\alpha)$. Mielivaltainen laajennuksen $\mathbb{Q}[x]/\langle x^2-2\rangle$ alkio on muotoa $\sum_j q_j x^j + \langle x^2-2\rangle$, missä $\sum_j q_j x^j$ on jokin $\mathbb{Q}$-kertoiminen polynomi. Jokaiselle laajennuksen $\mathbb{Q}[x]/\langle x^2-2\rangle$ alkiolle kuitenkin pätee

$$\begin{aligned}\sum_j q_j x^j + \langle x^2-2\rangle &= \sum_j (q_j x^j + \langle x^2-2\rangle) \\ &= \sum_j (q_j + \langle x^2-2\rangle)(x^j + \langle x^2-2\rangle) \\ &= \sum_j (q_j + \langle x^2-2\rangle)(x + \langle x^2-2\rangle)^j,\end{aligned}$$

missä $x + \langle x^2-2\rangle = \alpha$, joten

$$\sum_j (q_j + \langle x^2-2\rangle)(x + \langle x^2-2\rangle)^j \in K'(\alpha).$$

On siis oltava $K'(\alpha) = \mathbb{Q}[x]/\langle x^2-2\rangle$, joten laajennus $\mathbb{Q}[x]/\langle x^2-2\rangle$ on polynomin x^2-2 juurikunta. Lauseen 4.6 perusteella pätee siis $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}[x]/\langle x^2-2\rangle$.

Juurikuntien isomorfisuus paljastaa myös yhteyden äärellisten laajennusten, normaalien laajennusten ja juurikuntien välillä. Juurikunta aina äärellinen laajennus, mutta äärellinen laajennus on jonkin polynomin juurikunta vain jos se on normaali.

Lause 4.9. *Laajennus L/K on normaali ja äärellinen, jos ja vain jos L on jonkin K-kertoimisen polynomin juurikunta.*

Todistus. Oletetaan, että laajennus L/K on normaali ja äärellinen. Lauseen 2.19 nojalla $L = K(\alpha_1, \ldots, \alpha_r)$ joillakin alkioilla $\alpha_1, \ldots, \alpha_r \in L$, jotka ovat algebrallisia kunnan K suhteen. Olkoon $m_i(x) \in K[x]$ alkion α_i minimipolynomi kunnan K suhteen ja olkoon $f(x) = m_1(x) \cdots m_r(x) \in K[x]$. Kukin minimipolynomi $m_i(x)$ on jaoton renkaassa $K[x]$, ja kullakin niistä on ainakin yksi juuri α_i laajennuskunnassa L, joten normaalin laajennuksen määritelmän nojalla kukin $m_i(x)$ voidaan ilmaista ensimmäisen asteen polynomien tulona kunnassa L. Näin ollen myös $f(x)$ voidaan esittää ensimmäisen asteen termien tulona kunnassa L, ja koska alkiot α_i ovat polynomin $f(x)$ juuret, on $L = K(\alpha_1, \ldots, \alpha_r)$ polynomin $f(x)$ juurikunta.

Kääntäen, oletetaan, että L on jonkin polynomin $g(x) \in K[x]$ juurikunta. Juurikunnan määritelmän yhteydessä todettiin, että juurikunta on aina äärellinen laajennus, joten riittää osoittaa laajennuksen L/K olevan normaali. Tehdään tämä näyttämällä, että mikä tahansa jaoton K-kertoiminen polynomi, jolla on ainakin yksi juuri kunnassa L, jakautuu ensimmäisen asteen termien tuloksi kunnassa L.

Olkoon $f(x) \in K[x]$ jaoton polynomi, ja olkoot α_1, α_2 sen juuria jossain polynomin $f(x)$ juurikunnassa. Pyritään osoittamaan, että jos $\alpha_1 \in L$, niin myös $\alpha_2 \in L$, jolloin laajennus L/K on siis normaali. Osoitetaan ensin, että $[L(\alpha_1) : L] = [L(\alpha_2) : L]$. Molemmilla $j = 1, 2$ pätee lauseen 2.5 perusteella

$$[L(\alpha_j) : L][L : K] = [L(\alpha_j) : K],$$

joten

$$[L(\alpha_j) : L] = \frac{[L(\alpha_j) : K]}{[L : K]}, \tag{4.10}$$

ja vastaavasti

$$[L(\alpha_j) : K] = [L(\alpha_j) : K(\alpha_j)][K(\alpha_j) : K]. \tag{4.11}$$

Polynomi $f(x)$ oletettiin jaottomaksi, ja kuitenkin sen juurten α_1 ja α_2 minimipolynomit jakavat sen lauseen 2.12 perusteella. Minimipolynomien asteiden on siis oltava samat ja erityisesti niiden on oltava samat kuin polynomin $f(x)$ asteen, joten lausetta 2.16 soveltaen saadaan $[K(\alpha_1) : K] = [K(\alpha_2) : K]$.

Kunta L oletettiin polynomin $g(x) \in K[x]$ juurikunnaksi. Koska kuitenkin $K \subset K(\alpha_j)$, niin laajennuksen $L(\alpha_j)$ on vastaavasti oltava polynomin $g(x)$ juurikunta kunnan $K(\alpha_j)$ suhteen. Alkiot α_1 ja α_2 ovat jaottoman polynomin $f(x) \in K[x]$ juuria, joten soveltamalla lausetta 4.1 identtiseen kuvaukseen $\mathrm{id}\colon K \to K$ saadaan $K(\alpha_1) \cong K(\alpha_2)$. Polynomin $g(x)$ juurikuntina laajennukset $L(\alpha_1)/K(\alpha_1)$ ja $L(\alpha_2)/K(\alpha_2)$ ovat siten lauseen 4.6 nojalla isomorfiset, joten

$$[L(\alpha_1) : K(\alpha_1)] = [L(\alpha_2) : K(\alpha_2)].$$

Sijoittamalla näin saadut tiedot yhtälöihin (4.10) ja (4.11) saadaan

$$\begin{aligned}
[L(\alpha_1) : L] &= \frac{[L(\alpha_1) : K]}{[L : K]} \\
&= \frac{[L(\alpha_1) : K(\alpha_1)][K(\alpha_1) : K]}{[L : K]} \\
&= \frac{[L(\alpha_2) : K(\alpha_2)][K(\alpha_2) : K]}{[L : K]} \\
&= \frac{[L(\alpha_2) : K]}{[L : K]} \\
&= [L(\alpha_2) : L].
\end{aligned}$$

Oletetaan nyt, että $\alpha_1 \in L$. Tällöin $[L(\alpha_1) : L] = 1$, joten aiemman päättelyn nojalla

$$[L(\alpha_2) : L] = [L(\alpha_1) : L] = 1,$$

mistä seuraa, että $\alpha_2 \in L$. Toisin sanoen, jos yksi polynomin $f(x)$ juurista on kunnassa L, sen kaikki juuret ovat kunnassa L, jolloin se myös jakautuu ensimmäisen asteen tekijöiksi kunnassa L. Laajennus L/K on siis normaali. □

Luku 5

Galois'n ryhmä

Luvussa 4 käsiteltiin yleisiä kuntaisomorfismeja, mutta todellisen avaimen polynomien ratkeavuuteen tarjoavat niin kutsutut automorfismit eli sellaiset isomorfismit, jotka kuvaavat tarkasteltavan kunnan itselleen. Jos laajennuskunnan automorfismi kiinnittää laajennuksen lähtökunnan, se itse asiassa permutoi niiden polynomien juuria, joiden kertoimet ovat lähtökunnassa. Kaiken kukkuraksi automorfismit muodostavat peräti juurten permutaatioryhmiä, jolloin voidaankin käyttää yleistä ryhmien teoriaa näiden permutaatioryhmien ja ennen kaikkea niiden sisäisen rakenteen tutkimiseen.

Automorfismien muodostamat ryhmät ovat niinkin järeitä työkaluja, ettei niitä ei sovi rajoittaa polynomien juurten permutaatioiden tutkimiseen. Luvussa määritelläänkin tämä Galois'n ryhmäksi kutsuttu käsite yleisemmin myös kuntalaajennuksille. Yhteys kuntalaajennusten ja niitä vastaavien juurten permutaatioiden välillä konkretisoituu viimeistään luvun lopussa, kun osoitetaan, että kuntalaajennuksen aste voidaan päätellä suoraan laajennukseen liittyvän Galois'n ryhmän koosta ja päinvastoin.

5.1 Automorfismit

Aloitetaan määrittelemällä automorfismit täsmällisesti.

Määritelmä 5.1. Olkoon L kunta. Isomorfismia $\sigma\colon L \to L$, joka kuvaa kunnan L itselleen, kutsutaan *automorfismiksi*.

Oletetaan, että L on kunnan K laajennus. Jos kuvaus σ pitää kunnan K alkiot paikallaan eli jos $\sigma(k) = k$ kaikilla $k \in K$, niin sanotaan, että kuvaus σ *kiinnittää* kunnan K. Tällöin sanotaan myös, että kuvaus σ on K-*automorfismi* kunnassa L.

Laajennuskunnan automorfismit soveltuvat erinomaisesti polynomien juurten tutkimiseen. Seuraava lause on itsessäänkin varsin huomionarvoinen, mutta todellisuudessa se on vasta esimakua automorfismien käyttökelpoisuudesta.

Lause 5.2. *Olkoon L kunnan K laajennus. Jos $f(x) \in K[x]$, niin kunnan L mikä tahansa K-automorfismi kuvaa kuntaan L sisältyvät polynomin $f(x)$ juuret toisilleen.*

Todistus. Olkoon σ on kunnan L jokin K-automorfismi. Oletetaan, että $\alpha \in L$ on polynomin $f(x) = a_0 + a_1 x + \cdots + a_n x^n \in K[x]$ juuri ja osoitetaan, että myös $\sigma(\alpha)$ on polynomin $f(x)$ juuri. Jos $\alpha \in K$, niin

$$f(\sigma(\alpha)) = f(\alpha) = 0,$$

sillä K-automorfismina kuvaus σ kiinnittää alkion α. Jos puolestaan $\alpha \in L \setminus K$, niin K-automorfismin ominaisuuksien perusteella

$$\begin{aligned} f(\sigma(\alpha)) &= a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n \\ &= \sigma(a_0) + \sigma(a_1\alpha) + \cdots + \sigma(a_n\alpha^n) \\ &= \sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \sigma(f(\alpha)) \\ &= \sigma(0) \\ &= 0. \end{aligned}$$

□

Automorfismit pääsevät toden teolla oikeuksiinsa vasta juurikunnissa. Olkoon L jonkin polynomin $f(x) \in K[x]$ juurikunta. Juurikunnan määritelmän yhteydessä todettiin, että juurikunta on aina algebrallinen laajennus, joten mikä tahansa alkio $\alpha \in L$ on jonkin K-kertoimisen polynomin juuri. Nyt lauseen 5.2 perusteella siis tiedetään, että mielivaltainen K-automorfismi lähettää alkion α saman polynomin jollekin juurelle. Tämä itsessäänkin valottaa automorfismien toimintaa, mutta mielivaltaisten alkioiden ja polynomien tutkiminen ei vielä auta rajaamaan tarkasteluamme, sillä laajennuskunnassa voi olla äärettömän monta alkiota ja kukin niistä voi olla usean polynomin juuri.

Hedelmällisemmäksi osoittautuukin ottaa lähtökohdaksi juuri se polynomi $f(x)$, jonka juurikunta L on. Määritelmänsä mukaisesti juurikunta L voidaan esittää muodossa $L = K(\alpha_1, \ldots, \alpha_n)$, missä alkiot $\alpha_1, \ldots, \alpha_n \in L$ ovat polynomin $f(x)$ juuret. Tuloksen (3.5) perusteella tiedetään nyt, että jokainen juurikunnan alkio voidaan puolestaan esittää muodossa

$$\sum_i k_i \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n},$$

missä $k_i \in K$ ja $i = (i_1, \ldots, i_n)$. Olkoon nyt $\sigma\colon L \to L$ jokin K-automorfismi. Tällöin

millä tahansa juurikunnan alkiolla $\beta \in L$ pätee

$$\begin{aligned}
\sigma(\beta) &= \sigma(\sum_i k_i \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}) \\
&= \sum_i \sigma(k_i \alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}) \\
&= \sum_i k_i \sigma(\alpha_1^{i_1} \alpha_2^{i_2} \cdots \alpha_n^{i_n}) \\
&= \sum_i k_i \sigma(\alpha_1^{i_1}) \sigma(\alpha_2^{i_2}) \cdots \sigma(\alpha_n^{i_n}) \\
&= \sum_i k_i \sigma(\alpha_1)^{i_1} \sigma(\alpha_2)^{i_2} \cdots \sigma(\alpha_n)^{i_n},
\end{aligned}$$

joten mielivaltainen juurikunnan K-automorfismi σ määräytyy siis kokonaan alkioiden α_i kuvautumisesta. Kukin α_i on kuitenkin polynomin $f(x)$ juuri, joten polynomin $f(x)$ juurikunnan automorfismit ovat näin ollen kokonaan tulkittavissa polynomin $f(x)$ juurten permutaatioina.

Lähtökunnan kiinnittävien automorfismien tulkitseminen polynomin juurten permutaatioina on merkittävä linkki polynomien teorian ja kuntalaajennusten välillä. Erityisen käyttökelpoiseksi tämän linkin tekee kuitenkin sen yhteys ryhmäteoriaan: laajennuksen lähtökunnan kiinnittävät automorfismit muodostavat ryhmän.

Lause 5.3. *Olkoon L kunnan K laajennus. Kunnan L kaikkien K-automorfismien joukko muodostaa ryhmän, kun laskutoimituksena on kuvausten yhdistäminen.*

Todistus. Olkoot $\sigma, \tau \colon L \to L$ molemmat K-automorfismeja. On suoraviivaista osoittaa, että $\sigma \circ \tau$ on automorfismi, ja jos $k \in K$, niin $(\sigma \circ \tau)(k) = \sigma(\tau(k)) = \sigma(k) = k$, joten $\sigma \circ \tau$ (ja vastaavasti myös $\tau \circ \sigma$) on lisäksi K-automorfismi. Kuvausten yhdistäminen on tunnetusti liitännäinen laskutoimitus, ja sen neutraalialkio (identtinen kuvaus) on selvästi K-automorfismi. Automorfismi on bijektiona kääntyvä, joten K-automorfismille σ on olemassa käänteiskuvaus σ^{-1}, joka on myös automorfismi. Se on lisäksi K-automorfismi, sillä $\sigma^{-1}(k) = \sigma^{-1}(\sigma(k)) = k$ kaikilla $k \in K$. □

Lauseen 5.3 automorfismiryhmä on peräti niin keskeinen, että se on nimetty *Galois'n ryhmäksi*. Myöhemmin osoitetaan, että polynomin Galois'n ryhmän sisäisestä rakenteesta saadaan välttämätön ja riittävä ehto polynomin juurtamalla ratkeavuudelle. Moderni tapa määritellä polynomin Galois'n ryhmä määrittelee ensin kuitenkin *laajennuksen* Galois'n ryhmän.

Määritelmä 5.4. Laajennuksen L/K *Galois'n ryhmä* $\mathrm{Gal}(L/K)$ on kaikkien niiden kunnan L automorfismien joukko, jotka kiinnittävät kunnan K.

Määritelmä 5.5. Olkoon $f(x) \in K[x]$ jokin polynomi ja L sen juurikunta. Polynomin $f(x)$ *Galois'n ryhmä* on laajennuksen L/K Galois'n ryhmä.

Polynomin Galois'n ryhmän määritelmästä nähdään, että jos jokin laajennus on polynomin juurikunta, laajennuksen Galois'n ryhmä ja polynomin Galois'n ryhmä ovat sama asia. Galois'n ryhmän käsitteen yleistäminen juurten permutaatioista kuntalaajennuksiin auttaa toki soveltamaan Galois'n ryhmään liittyviä tuloksia myös juurikuntien ulkopuolella, mutta pääasiallinen syy tähän kuntalaajennuksia painottavaan lähestymistapaan on historiallinen. Galois itse pohjasi teoriansa puhtaasti polynomin juurten permutaatioille, mutta kuten [10] osoittaa, Galois'n lähestymistapa oli varsin monimutkainen ja hankala. Useimmat modernit esitykset pohjaavatkin pitkälti Artinin (ks. [1]) esittelemään kuntalaajennuksiin pohjautuvaan lähestymistapaan, joka on sekä teknisesti yksinkertaisempi että helpommin yleistettävä.

Esimerkki 5.6. Etsitään esimerkin 3.6 polynomin $f(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ Galois'n ryhmä. Esimerkissä todettiin, että polynomin $f(x)$ juurikunta on $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, joten polynomin $f(x)$ Galois'n ryhmä on samalla myös laajennuksen $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ Galois'n ryhmä.

Lauseen 5.2 yhteydessä näytettiin, että Galois'n ryhmän alkiot ovat polynomin $f(x)$ juurten permutaatioita. Polynomilla $f(x)$ on tasan neljä juurta $\sqrt{2}, -\sqrt{2}, \sqrt{3}$ ja $-\sqrt{3}$, joten sen Galois'n ryhmä koostuu neljän alkion permutaatioista ja on siten symmetrisen ryhmän S_4 aliryhmä. Selvitetään, millaiset permutaatiot voivat olla polynomin $f(x)$ Galois'n ryhmän alkioita. Lauseen 5.2 perusteella tiedetään, että Galois'n ryhmän permutaation on aina kuvattava minkä tahansa polynomin juuret toisilleen. Näin ollen esimerkiksi $\sqrt{2}$ ei voi kuvautua juurelle $\sqrt{3}$, sillä $\sqrt{3}$ ei ole polynomin $x^2 - 2 \in \mathbb{Q}[x]$ juuri. Eliminoimalla vastaavasti muut mahdottomat permutaatiot päädytään siihen lopputulokseen, että polynomin $f(x)$ (ja samalla myös laajennuksen $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$) Galois'n ryhmän kaikki alkiot ovat seuraavat juurten $\pm\sqrt{2}, \pm\sqrt{3}$ permutaatiot:

$$\epsilon = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \end{pmatrix}, \qquad \rho = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{2} & \sqrt{3} & -\sqrt{3} \end{pmatrix},$$

$$\sigma = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ \sqrt{2} & -\sqrt{2} & -\sqrt{3} & \sqrt{3} \end{pmatrix} \quad \text{ja} \quad \tau = \begin{pmatrix} \sqrt{2} & -\sqrt{2} & \sqrt{3} & -\sqrt{3} \\ -\sqrt{2} & \sqrt{2} & -\sqrt{3} & \sqrt{3} \end{pmatrix}.$$

Polynomin $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$ voidaan puolestaan osoittaa olevan laajennuksen $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$ minimipolynomi, joten lauseen 2.16 nojalla laajennuksen $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ aste on 4. Pian käsiteltävässä lauseessa 5.12 osoitetaankin, että kuntalaajennuksen aste aina sama kuin sitä vastaavan Galois'n ryhmän koko ja päinvastoin.

5.2 Galois'n ryhmän koko

Laajennuksen L/K Galois'n ryhmässä $\mathrm{Gal}(L/K)$ ovat kaikki ne kunnan L automorfismit, jotka kiinnittävät *ainakin* kunnan K. Yksittäinen Galois'n ryhmän K-automorfismi voi siis kiinnittää alkioita myös kunnan K ulkopuolelta: esimerkiksi identtinen kuvaus $\mathrm{id}\colon L \to L$ kiinnittää koko laajennuskunnan L.

Galois'n ryhmän jonkin osajoukon kiinnittämä kunnan L osajoukko voikin vastaavasti olla suurempi kuin K. Erityisen kiinnostaviksi osoittautuvat Galois'n ryhmän *aliryhmät*, sillä mikä tahansa kunnan L automorfismiryhmän kiinnittämä kunnan L osajoukko muodostaa itse asiassa kunnan, jota kutsutaan kyseisen aliryhmän *kiintokunnaksi*. Yhteys Galois'n ryhmän aliryhmien ja niiden kiintokunnista muodostettujen laajennusten välillä nousee luvussa 6 todistettavan Galois'n teorian peruslauseen keskeisimmäksi sisällöksi.

Määritelmä 5.7. Olkoon S ryhmä kunnan L automorfismeja. Ryhmän S *kiintokunta* on $\mathrm{Fix}(S) = \{a \in L : \sigma(a) = a \text{ kaikilla } \sigma \in S\}$, eli kaikkien niiden kunnan L alkioiden joukko, jotka jokainen ryhmän S automorfismi kiinnittää.

Kiintokunnat ovat avainasemassa, kun myöhemmin tarvitsemme sisäkkäisten kuntalaajennusten muodostamia torneja. Kullakin tornin välilaajennuksella on oma Galois'n ryhmänsä, jonka alkiot kiinnittävät välilaajennuksen lähtökunnan Galois'n ryhmän määritelmän mukaisesti. Erityisen käyttökelpoisia ovat sellaiset seuraavassa luvussa käsiteltävät laajennukset, joiden kiintokunta on täsmälleen välilaajennuksen lähtökunta.

Välilaajennusten Galois'n ryhmien ja kiintokuntien käsittelyä helpottaa se, että Galois'n ryhmän koko ja sitä vastaavan kiintokunnan laajennuksen aste vastaavat täysin toisiaan. Tämän todistaminen vaatii kuitenkin teknisiä apuneuvoja.

Määritelmä 5.8. Ryhmän G *karakteeri* kunnassa L on mikä tahansa ryhmähomomorfismi $\sigma\colon G \to L^*$, missä L^* on kunnan L kertolaskuryhmä $(L \setminus \{0\}, \cdot)$.

Olkoon $\sigma\colon L \to L$ jokin K-automorfismi. Tällöin kaikilla alkioilla $a, b \in L$ pätee $\sigma(ab) = \sigma(a)\sigma(b)$, joten kun rajoitutaan tarkastelemaan kertolaskuryhmää L^*, kuvaus $\sigma\colon L^* \to L^*$ on ryhmähomomorfismi. Kunnan L jokainen K-automorfismi on siis tulkittavissa kunnan kertolaskuryhmän karakteerina itselleen, kun yllä olevassa määritelmässä asetetaan $G = L^*$. Tätä tulkintaa hyödynnetään seuraavissa todistuksissa.

Lemma 5.9. *Olkoon $S = \{\sigma_i\colon G \to L^*\}$ joukko ryhmän G eri karakteereja kunnassa L. Tällöin joukko S on vapaa kunnassa L, eli jos joukossa S on n alkiota ja on olemassa sellaiset kertoimet $l_1, \ldots, l_n \in L$, että*

$$\sum_{i=1}^{n} l_i \sigma_i(g) = 0$$

kaikilla $g \in G$, niin on oltava $l_i = 0$ kaikilla i.

Todistus. Oletetaan, että $S = \{\sigma_i : i = 1, \ldots, n\}$ on sellainen joukko ryhmän G eri karakteereja kunnassa L, että se ei ole vapaa. Tällöin on siis olemassa sellaiset kertoimet $l_1, \ldots, l_n \in L$, että

$$\sum_{i=1}^{n} l_i \sigma_i(g) = 0$$

kaikilla $g \in G$, mutta ainakin yksi kertoimista l_i ei ole nolla. Olkoon $l_1, \ldots, l_m$ pienin mahdollinen kokoelma nollasta poikkeavia kertoimia l_i.

Olkoot $\sigma_1, \sigma_2 \in S$ kaksi eri karakteeria. Tällöin on siis olemassa jokin sellainen $h \in G$, että $\sigma_1(h) \neq \sigma_2(h)$. Olkoon nyt $g \in G$. Tarkastellaan lauseketta

$$\sum_{i=1}^{m} l_i \sigma_1(h) \sigma_i(g) - \sum_{i=1}^{m} l_i \sigma_i(h) \sigma_i(g). \tag{5.10}$$

Alkioiden $l_1, \ldots, l_m$ valinnasta seuraa, että erotuksen vasemmanpuoleiselle summalausekkeelle pätee

$$\sum_{i=1}^{m} l_i \sigma_1(h) \sigma_i(g) = \sigma_1(h) \sum_{i=1}^{m} l_i \sigma_i(g) = 0,$$

ja toiselle termille puolestaan pätee

$$\sum_{i=1}^{m} l_i \sigma_i(h) \sigma_i(g) = \sum_{i=1}^{m} l_i \sigma_i(hg) = 0$$

kaikilla $g \in G$, joten erotuksen (5.10) on oltava nolla. Näin ollen

$$\begin{aligned}
&\sum_{i=1}^{m} l_i \sigma_1(h) \sigma_i(g) - \sum_{i=1}^{m} l_i \sigma_i(h) \sigma_i(g) \\
=& \sum_{i=1}^{m} l_i (\sigma_1(h) - \sigma_i(h)) \sigma_i(g) \\
=& \; l_1(\sigma_1(h) - \sigma_1(h))\sigma_1(g) + \sum_{i=2}^{m} l_i (\sigma_1(h) - \sigma_i(h)) \sigma_i(g) \\
=& \sum_{i=2}^{m} (l_i(\sigma_1(h) - \sigma_i(h))) \sigma_i(g) \qquad (5.11) \\
=& \; 0
\end{aligned}$$

kaikilla $g \in G$. Nyt lausekkeen (5.11) kaikki kertoimet $l_i(\sigma_1(h) - \sigma_i(h))$ ovat kunnassa L ja ne eivät kaikki ole nollia, sillä aiemmin todettiin, että ainakin $\sigma_1(h) - \sigma_2(h) \neq 0$. Lausekkeessa (5.11) on kuitenkin vain $m - 1$ termiä, mikä on ristiriita, sillä m oletettiin pienimmäksi määräksi tällaisia kertoimia. □

Nyt voidaan todistaa luvun keskeisin tulos, joka osoittaa esimerkissä 5.6 mainitun yhteyden Galois'n ryhmän koon ja kuntalaajennuksen asteen välillä itse asiassa kahdesta eri näkökulmasta. Jos nimittäin on annettu äärellinen ryhmä eri automorfismeja (esimerkiksi jokin Galois'n ryhmä), niin ryhmän koko saadaan sen kiintokunnan laajennuksen asteesta. Toisaalta lause kertoo, että annetun laajennuksen aste saadaan etsimällä ensin se automorfismien ryhmä, joiden kiintokunta on laajennuksen lähtökunta, ja selvittämällä sitten kyseisen ryhmän koko.

Lisäksi lause 5.12 osoittaa, että laajennuksen L/K Galois'n ryhmä on *ainut* kunnan L automorfismien ryhmä, jonka kiintokunta on K. Minkä tahansa Galois'n ryhmän $\mathrm{Gal}(L/K)$ aidon aliryhmän kiintokunnan on siis oltava jokin muu kunta. Kaikki ryhmän $\mathrm{Gal}(L/K)$ alkiot kuitenkin kiinnittävät kunnan K, joten Galois'n ryhmän aliryhmän kiintokunnan on oltava jokin kunnan K laajennus.

Lause 5.12. *Olkoon L kunnan K äärellinen laajennus. Jos G on äärellinen ryhmä kunnan L eri automorfismeja ja $K = \mathrm{Fix}(G)$, niin $G = \mathrm{Gal}(L/K)$ ja $[L : K] = |G|$.*

Todistus. Olkoon $|G| = n$, jolloin voidaan merkitä $G = \{\sigma_i : i = 1, \ldots, n\}$. Merkitään lisäksi $d = [L : K]$. Osoitetaan ensin, että $n = d$.

Oletetaan, että $n > d$. Olkoon joukko $\{l_1, \ldots, l_d\}$ laajennuksen L/K kanta. Tarkastellaan yhtälöryhmää

$$\begin{bmatrix} \sigma_1(l_1) & \cdots & \sigma_n(l_1) \\ \vdots & \ddots & \vdots \\ \sigma_1(l_d) & \cdots & \sigma_n(l_d) \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = 0.$$

Koska $n > d$, niin yhtälöryhmässä on enemmän tuntemattomia kuin yhtälöitä, joten sille löytyy jokin epätriviaali ratkaisu $x_1, \ldots, x_n \in L$, missä siis ainakin jokin $x_i \neq 0$.

Olkoon $\alpha \in L$. Tällöin kannan $\{l_1, \ldots, l_d\}$ avulla ilmaistuna $\alpha = \sum_{j=1}^{d} k_j l_j$ joillakin $k_j \in K$. Ryhmän G kuvaukset kiinnittävät kunnan K, joten kaikilla i, j pätee $\sigma_i(k_j) = k_j$. Nyt

$$\begin{aligned} \sum_{i=1}^{n} x_i \sigma_i(\alpha) &= \sum_{i=1}^{n} x_i \sigma_i \left(\sum_{j=1}^{d} k_j l_j \right) = \sum_{i=1}^{n} x_i \sum_{j=1}^{d} \sigma_i(k_j l_j) = \sum_{i=1}^{n} \sum_{j=1}^{d} x_i k_j \sigma_i(l_j) \\ &= \sum_{j=1}^{d} k_j \sum_{i=1}^{n} x_i \sigma_i(l_j), \end{aligned}$$

missä $x_1, \ldots, x_n$ on kuitenkin edellä mainittu yhtälöryhmän epätriviaali ratkaisu, joten

$$\sum_{j=1}^{d} k_j \sum_{i=1}^{n} x_i \sigma_i(l_j) = \sum_{j=1}^{d} k_j \cdot 0 = 0.$$

Mielivaltaisella kunnan L alkiolla α pätee siis $\sum_{i=1}^{n} x_i \sigma_i(\alpha) = 0$, vaikka ainakin yksi alkioista x_i ei ole nolla. Tämä on kuitenkin ristiriita, sillä kuvausten σ_i joukko on kokoelma ryhmän L^* karakteereja ja siten vapaa kunnassa L lemman 5.9 nojalla. On siis oltava $n \leq d$.

Oletetaan seuraavaksi, että $n < d$. Olkoon σ_1 ryhmän G neutraalialkio eli identtinen kuvaus. Olkoon $\{l_1, \ldots, l_{n+1}\}$ sellainen joukko kunnan L alkioita, että se on vapaa kunnassa K. Tarkastellaan yhtälöryhmää

$$\begin{bmatrix} \sigma_1(l_1) & \cdots & \sigma_1(l_{n+1}) \\ \vdots & \ddots & \vdots \\ \sigma_n(l_1) & \cdots & \sigma_n(l_{n+1}) \end{bmatrix} \begin{bmatrix} y_1 \\ \vdots \\ y_{n+1} \end{bmatrix} = 0. \tag{5.13}$$

Tälläkin yhtälöryhmällä on ainakin yksi epätriviaali ratkaisu $y_1, \ldots, y_{n+1} \in L$. Valitaan kaikista mahdollisista epätriviaaleista ratkaisuista se, jolla on pienin määrä s nollasta poikkeavia termejä y_j. On siis olemassa sellaiset nollasta poikkeavat alkiot $y_j \in L$, että

$$\sum_{j=1}^{s} y_j \sigma_i(l_j) = 0 \tag{5.14}$$

kaikilla σ_i. Voidaan olettaa, että $y_s = 1$, sillä yhtälö (5.14) voidaan tarvittaessa jakaa alkiolla y_s.

Kaikki alkiot y_i eivät voi olla lähtökunnassa K, sillä tällöin pätisi

$$0 = \sum_{j=1}^{s} y_j \sigma_i(l_j) = \sum_{j=1}^{s} \sigma_i(y_j l_j) = \sigma\left(\sum_{j=1}^{s} y_j l_j\right),$$

joten olisi oltava $\sum_{j=1}^{s} y_j l_j = 0$ eli joukko $\{l_j\}$ ei olisikaan vapaa. Voidaan siis olettaa, että $y_1 \in L \setminus K$. Merkitään

$$\lambda_i = \sum_{j=1}^{s} y_j \sigma_i(l_j) \in L.$$

Koska $y_s = 1$, niin

$$\lambda_i = \sum_{j=1}^{s} y_j \sigma_i(l_j) = \sum_{j=1}^{s-1} y_j \sigma_i(l_j) + \sigma_i(l_s) = 0 \tag{5.15}$$

kaikilla i.

Kunta K on ryhmän G kiintokunta, joten koska $y_1 \notin K$, on oltava jokin $\sigma_k \in G$, jolla $\sigma_k(y_1) \neq y_1$. Lisäksi ryhmän ominaisuuksien perusteella kaikilla ryhmän G alkioilla σ_i on olemassa jokin σ_m, jolla $\sigma_k\sigma_m = \sigma_i$. Sijoittamalla alkio $\lambda_m \in L$ yhtälössä (5.15) esitetyssä muodossa automorfismiin σ_k saadaan

$$\sigma_k(\lambda_m) = \sigma_k\left(\sum_{j=1}^{s-1} y_j\sigma_m(l_j) + \sigma_m(l_s)\right) = \sum_{j=1}^{s-1} \sigma_k(y_j)\sigma_i(l_j) + \sigma_i(l_s) \tag{5.16}$$

kaikilla i. Lausekkeen (5.16) arvon on kuitenkin oltava nolla, sillä $\lambda_m = 0$ ja siten myös $\sigma_k(\lambda_m) = \sigma_k(0) = 0$. Yhdistämällä yhtälöiden (5.15) ja (5.16) tiedot saadaan siis

$$\lambda_i - \sigma_k(\lambda_m) = \sum_{j=1}^{s-1} y_j\sigma_i(l_j) + \sigma_i(l_s) - \left(\sum_{j=1}^{s-1} \sigma_k(y_j)\sigma_i(l_j) + \sigma_i(l_s)\right) = 0 - 0 = 0,$$

joten

$$\begin{aligned} &\sum_{j=1}^{s-1} y_j\sigma_i(l_j) + \sigma_i(l_s) - \left(\sum_{j=1}^{s-1} \sigma_k(y_j)\sigma_i(l_j) + \sigma_i(l_s)\right) \\ &= \sum_{j=1}^{s-1} (y_j - \sigma_k(y_j))\sigma_i(l_j) = 0 \end{aligned} \tag{5.17}$$

kaikilla i. Aiemmin kuitenkin todettiin, että automorfismille σ_k pätee $y_1 - \sigma_k(y_1) \neq 0$, joten yhtälön (5.17) lineaarikombinaation kertoimista ainakin yksi ei ole nolla. On siis saatu yhtälöryhmälle (5.13) ratkaisu, jossa on vähemmän kuin s nollasta poikkeavaa termiä. Tämä on kuitenkin ristiriita, sillä s oletettiin pienimmäksi määräksi tällaisia termejä. On siis oltava $n \geq d$, ja edelleen $n = d$.

Osoitetaan vielä, että $G = \mathrm{Gal}(L/K)$. Ryhmä G koostuu K-automorfismeista kunnassa L, joten $G \subset \mathrm{Gal}(L/K)$. Edellä kuitenkin osoitettiin, että $|G| = [L : K]$ ja vastaavalla päättelyllä voidaan osoittaa myös $|\mathrm{Gal}(L/K)| = [L : K]$, joten on oltava $G = \mathrm{Gal}(L/K)$. □

Luku 6

Galois'n yhteys

Polynomin juuret sisältävälle kuntalaajennukselle voidaan määritellä Galois'n ryhmä, joka koostuu polynomin juurten permutaatioista. Polynomin juuria voidaan kuitenkin lisätä sen kerroinkuntaan monessa eri järjestyksessä, eli toisin sanottuna laajennukselle voidaan määritellä useita erilaisia välilaajennuksia. Laajennuksen avaaminen välilaajennusten torniksi mahdollistaakin laajennuksen sisäisen rakenteen tarkan tutkimisen, minkä osoitetaan myöhemmissä luvuissa kertovan kaiken tarvittavan polynomien ratkeavuudesta.

Laajennuksen Galois'n ryhmä voidaan vastaavasti pilkkoa pienempiin osiin esimerkiksi tutkimalla sen aliryhmiä, mutta vielä ei ole selvää, miten välilaajennukset ja aliryhmät kytkeytyvät toisiinsa. Vastauksen ongelmaan antaa tässä luvussa todistettava Galois'n teorian peruslause, joka määrittelee tarkan yksi–yhteen-vastaavuuden kuntalaajennuksen välilaajennusten ja Galois'n ryhmän aliryhmien välille. Lisäksi peruslause kertoo myös täsmälleen millaisia algebrallisia rakenteita nämä aliryhmät ja välilaajennukset muodostavat.

6.1 Galois'n laajennukset

Pian käsiteltävää Galois'n teorian peruslausetta 6.7 ei voida soveltaa mielivaltaisissa kuntalaajennuksissa. Peruslause edellyttää, että tutkittava laajennus on niin sanottu Galois'n laajennus.

Määritelmä 6.1. Algebrallista laajennusta L/K kutsutaan *Galois'n laajennukseksi*, jos lähtökunta K on suurin laajennuskunnan L alikunta, jonka laajennuskunnan L kaikki K-automorfismit kiinnittävät. Tällöin siis $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$.

Galois'n laajennuksen sanotaan usein olevan lyhyesti *Galois*. On hyvä huomata, että Galois'n laajennuksen algebrallisuudesta johtuen Galois'n laajennus on aina äärellinen,

mikä on suora seuraus lauseesta 2.19 ja pian todistettavan lauseen 6.4 kolmannesta kohdasta.

Määritelmä myös takaa, että Galois'n laajennuksessa L/K mille tahansa laajennuskunnan alkiolle $x \in L \setminus K$ löytyy jokin automorfismi, joka liikuttaa sitä. Kaikki alkiot, joille ei liikuttajaa löydy, ovat väistämättä kunnassa K.

Esimerkki 6.2. Tarkastellaan laajennusta $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$ ja sen Galois'n ryhmää. Laajennuksen minimipolynomi on $x^4-7 \in \mathbb{Q}[x]$, jonka juuret ovat $\pm\sqrt[4]{7}$ ja $\pm i\sqrt[4]{7}$. Näistä juurista kuitenkin vain $\sqrt[4]{7}$ ja $-\sqrt[4]{7}$ ovat laajennuskunnassa $\mathbb{Q}(\sqrt[4]{7})$, joten identtisen kuvauksen lisäksi ainut mahdollinen juurten permutaatio on $\sigma(\sqrt[4]{7}) = -\sqrt[4]{7}$, missä siis $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q})$.

Alkiolle $\sqrt[4]{7}$ kuitenkin pätee $(\sqrt[4]{7})^2 = \sqrt{7}$, joten on oltava $\sqrt{7} \in \mathbb{Q}(\sqrt[4]{7})$ ja erityisesti $\mathbb{Q}(\sqrt{7}) \subset \mathbb{Q}(\sqrt[4]{7})$. Olkoon nyt α jokin välikunnan $\mathbb{Q}(\sqrt{7})$ alkio. Lauseen 2.14 perusteella alkio α voidaan esittää muodossa $\sum_j q_j(\sqrt[4]{7})^j$, missä $q_j \in \mathbb{Q}$. Koska kuitenkin

$$\sigma(\sqrt{7}) = \sigma((\sqrt[4]{7})^2) = (\sigma(\sqrt[4]{7}))^2 = (-\sqrt[4]{7})^2 = \sqrt{7},$$

niin

$$\sigma(\alpha) = \sigma\Big(\sum_j q_j(\sqrt{7})^j\Big) = \sum_j q_j\sigma((\sqrt{7})^j) = \sum_j q_j(\sigma(\sqrt{7}))^j = \sum_j q_j(\sqrt{7})^j = \alpha,$$

joten kuvaus σ kiinnittää myös kunnan $\mathbb{Q}(\sqrt{7})$. Kunta $\mathbb{Q}$ ei siis ole pienin kunta, jonka kunnan $\mathbb{Q}(\sqrt[4]{7})$ kaikkien $\mathbb{Q}$-automorfismien joukko kiinnittää, joten laajennus $\mathbb{Q}(\sqrt[4]{7})/\mathbb{Q}$ ei ole Galois.

Yllä oleva esimerkki ei vielä paljasta, miten laajennuksen voidaan osoittaa olevan Galois, mutta viime luvussa todistetun lauseen 5.12 avulla voidaan johtaa suoraviivainen kriteeri Galois'n laajennusten tunnistamiseksi.

Korollaari 6.3. *Olkoon L kunnan K äärellinen laajennus. Laajennus L/K on Galois, jos ja vain jos* $|\mathrm{Gal}(L/K)| = [L : K]$.

Todistus. Oletetaan ensin, että laajennus L/K on Galois. Tällöin Galois'n laajennuksen määritelmän perusteella pätee $K = \mathrm{Fix}(\mathrm{Gal}(L/K))$, joten lauseesta 5.12 saadaan suoraan $|\mathrm{Gal}(L/K)| = [L : K]$.

Kääntäen, oletetaan, että $|\mathrm{Gal}(L/K)| = [L : K]$. Merkitään $M = \mathrm{Fix}(\mathrm{Gal}(L/K))$, ja osoitetaan, että tällöin $M = K$. Joukko $\mathrm{Gal}(L/K)$ on äärellinen ryhmä kunnan L eri automorfismeja, jonka kiintokunta on M, mutta lauseen 5.12 nojalla ainut tällainen ryhmä on $\mathrm{Gal}(L/M)$, joten on siis oltava $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)$. Jälleen lausetta 5.12 soveltamalla saadaan siis

$$[L : M] = |\mathrm{Gal}(L/M)| = |\mathrm{Gal}(L/K)| = [L : K].$$

Kuitenkin lauseen 2.5 nojalla

$$[L : K] = [L : M][M : K],$$

joten on oltava $[M : K] = 1$. Näin ollen $M = K$ eli laajennus L/K on Galois.

□

Ulkomuotonsa puolesta Galois'n laajennuksen määritelmä poikkeaa huomattavasti aiemmin käsitellyistä kuntalaajennusten tyypeistä. Seuraava, usein hyödynnetty lause kuitenkin osoittaa, että näennäisen poikkeavasta määritelmästään huolimatta Galois'n laajennukset kytkeytyvät suoraan muihin laajennustyyppeihin.

Lause korostaa myös separoituvuuden merkitystä. Separoituvan polynomin juuret ovat erillisiä, jolloin permutoitavien juurten määrä nähdään suoraan polynomin asteesta. Tällöin voidaan suoraan sanoa, että n-asteisen polynomin Galois'n ryhmä on symmetrisen ryhmän S_n aliryhmä.

Lause 6.4. *Olkoon L kunnan K äärellinen laajennus. Seuraavat väitteet ovat tällöin yhtäpitävät:*

1. *L/K on Galois'n laajennus.*
2. *L/K on normaali ja separoituva.*
3. *L on jonkin K-kertoimisen separoituvan polynomin juurikunta.*

Todistus. 1. $\Rightarrow$ 2. Oletetaan, että L/K on Galois'n laajennus. Osoitetaan ensin laajennuksen L/K olevan separoituva näyttämällä, että mielivaltaisen alkion $\alpha \in L$ minimipolynomi $m(x) \in K[x]$ on separoituva. Alkion α *Galois'n konjugaattien* joukon $\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}$ jokainen jäsen on minimipolynomin $m(x)$ juuri lauseen 5.2 nojalla. Konjugaattien joukko on siten äärellinen ja alkio α on yksi sen jäsenistä, sillä identtinen kuvaus on K-automorfismi, joka konjugoi alkion α itselleen.

Olkoot $\alpha_1, \ldots, \alpha_n \in L$ Galois'n konjugaattien joukon erilliset alkiot. Määritellään polynomi

$$f(x) = \prod_i (x - \alpha_i) \in L[x].$$

Tällöin kaikilla kuvauksilla $\tau \in \mathrm{Gal}(L/K)$ pätee $\tau(f(x)) = f(x)$, sillä kuvaus τ permutoi alkioita α_i lauseen 5.2 perusteella ja siten se korkeintaan muuttaa polynomin $f(x)$ termien järjestystä. Näin ollen ryhmän $\mathrm{Gal}(L/K)$ kuvaukset eivät muuta polynomin $f(x)$ kertoimia, joten polynomin $f(x)$ kertoimet ovat siis ryhmän $\mathrm{Gal}(L/K)$ kiintokunnassa. Laajennus L/K on kuitenkin Galois, joten sen kiintokunta on K. On siis oltava $f(x) \in K[x]$.

Polynomi $f(x)$ on siis K-kertoiminen polynomi, jonka eräs juuri on α, joten lauseen 2.12 perusteella alkion α minimipolynomi $m(x)$ jakaa polynomin $f(x)$. Alkiot $\alpha_1, \ldots, \alpha_n$ oletettiin kuitenkin erillisiksi, joten polynomilla $m(x)$ ei siten ole moninkertaisia juuria. Mielivaltaisesti valitun alkion $\alpha \in L$ minimipolynomi on siis separoituva, joten myös laajennus L/K on separoituva.

Osoitetaan vielä, että laajennus L/K on normaali. Olkoon $g(x) \in K[x]$ jaoton polynomi. Oletetaan, että polynomilla $g(x)$ on kunnassa L jokin juuri β. Osoitetaan, että tällöin polynomin $g(x)$ kaikki juuret ovat kunnassa L. Alkion β minimipolynomi $m_\beta(x) \in K[x]$ jakaa polynomin $g(x)$ lauseen 2.12 nojalla, mutta polynomi $g(x)$ on kuitenkin jaoton, joten on oltava $g(x) = km_\beta(x)$ jollain $k \in K$. Edellä osoitetun perusteella polynomi $m_\beta(x)$ jakautuu kuitenkin ensimmäisen asteen termien tuloksi kunnassa L, joten myös polynomin $g(x)$ on jakauduttava ensimmäisen asteen termien tuloksi kunnassa L. Polynomin $g(x)$ kaikki juuret ovat siis kunnassa L, joten laajennus L/K on normaali.

2. $\Rightarrow$ 3. Oletetaan, että laajennus L/K on normaali ja separoituva. Olkoon joukko $\{l_1, \ldots, l_n\}$ laajennuksen L/K kanta, ja olkoon $m_{l_i}(x) \in K[x]$ alkion l_i minimipolynomi. Olkoon nyt $f(x) \in K[x]$ kaikkien erillisten minimipolynomien $m_{l_i}(x)$ tulo. Osoitetaan, että $f(x)$ on etsimämme polynomi.

Osoitetaan ensin, että polynomi $f(x)$ on separoituva. Laajennus L/K oletettiin separoituvaksi, joten kukin minimipolynomi $m_{l_i}(x)$ on separoituva. Eri alkioiden minimipolynomien juuret ovat lisäksi erillisiä, joten polynomilla $f(x)$ ei myöskään ole moninkertaisia juuria eli se on separoituva.

Osoitetaan sitten, että laajennus L/K on polynomin $f(x)$ juurikunta. Laajennus L/K oletettiin normaaliksi, joten koska kullakin minimipolynomilla $m_{l_i}(x)$ on ainakin yksi juuri l_i kunnassa L, niiden kaikki juuret ovat kunnassa L. Näin ollen kukin minimipolynomi $m_{l_i}(x)$ jakautuu ensimmäisen asteen termien tuloksi kunnassa L, joten myös polynomi $f(x)$ jakautuu ensimmäisen asteen termien tuloksi kunnassa L. Lisäksi kannan $\{l_1, \ldots, l_n\}$ alkiot l_i ovat polynomin $f(x)$ juuria, joten mikä tahansa kunta, jossa $f(x)$ jakautuu ensimmäisen asteen termien tuloksi, sisältää väistämättä alkiot l_i lineaarikombinaatioineen. Alkiot l_i kuitenkin virittävät koko kunnan L, joten L on siis pienin polynomin $f(x)$ juuret sisältävä kunta. Kunta L on siis separoituvan polynomin $f(x)$ juurikunta.

3. $\Rightarrow$ 1. Oletetaan, että L on separoituvan polynomin $f(x) \in K[x]$ juurikunta. Tällöin polynomin $f(x)$ kaikki juuret ovat kunnassa L, mutta ei ole tietoa siitä, miten moni niistä on kunnassa K. Todistetaankin lause induktiolla sen suhteen, miten monta polynomin $f(x)$ juurista on kunnan K ulkopuolella laajennuskunnassa L.

Oletetaan ensin, että polynomin $f(x)$ juurista yksikään ei ole kunnan K ulkopuolella. Jos alkiot $\alpha_1, \ldots, \alpha_n$ ovat polynomin $f(x)$ juuret, niin juurikunta L voidaan esittää muodossa $L = K(\alpha_1, \ldots, \alpha_n)$. Oletuksesta $\alpha_1, \ldots, \alpha_n \in K$ kuitenkin seuraa väistämättä $K(\alpha_1, \ldots, \alpha_n) = K$, joten $L = K$. Laajennuksen L/K aste on tällöin yksi, joten ryhmässä $\mathrm{Gal}(L/K)$ on lauseen 5.12 nojalla vain yksi alkio eli identtinen kuvaus $\mathrm{id}\colon L \to L$. Nyt

siis $\mathrm{Fix}(\mathrm{Gal}(L/K)) = L = K$, joten laajennus L/K on Galois.

Oletetaan sitten, että väite pätee kaikilla $m < k \in \mathbb{N}$. Olkoot $\alpha_1, \ldots, \alpha_n$ jälleen polynomin $f(x)$ juuret, ja oletetaan, että niistä k kappaletta on joukossa $L \setminus K$. Jaetaan polynomi $f(x)$ jaottomien termien tuloksi renkaassa $K[x]$, jolloin siis

$$f(x) = f_1(x)f_2(x)\cdots f_m(x)$$

joillakin $f_j(x) \in K[x]$. Polynomin $f(x)$ juurista ainakin yksi ei oletuksen nojalla ole kunnassa K, joten voidaan olettaa, että $\deg(f_1(x)) = s > 1$. Olkoon nyt $\alpha_1 \in L$ polynomin $f_1(x)$ jokin juuri. Polynomi $f_1(x)$ on jaoton, mutta lauseen 2.12 nojalla alkion α_1 minimipolynomi kuitenkin jakaa sen, joten minimipolynomin ja polynomin $f_1(x)$ on oltava samaa astetta. Näin ollen $[K(\alpha_1) : K] = \deg(f_1(x)) = s$.

Polynomin $f(x)$ juurista k kappaletta on kunnan K ulkopuolella, mutta ainakin yksi niistä on laajennuksessa $K(\alpha_1)$, joten juurista vähemmän kuin k on laajennuksen $K(\alpha_1)$ ulkopuolella. Kuitenkin $f(x) \in K(\alpha_1)[x]$ ja L on polynomin $f(x)$ juurikunta myös kunnan $K(\alpha_1)$ suhteen, joten induktio-oletuksen nojalla laajennus $L/K(\alpha_1)$ on Galois, mistä seuraa, että $\mathrm{Fix}(\mathrm{Gal}(L/K(\alpha_1))) = K(\alpha_1)$.

Polynomi $f(x)$ oletettiin kuitenkin separoituvaksi, joten myös polynomin $f_1(x)$ juuret α_i ovat erillisiä. Lisäksi polynomi $f_1(x)$ oletettiin jaottomaksi renkaassa $K[x]$, joten lauseen 4.1 nojalla on olemassa isomorfismit $\phi_i \colon K(\alpha_1) \to K(\alpha_i)$, joilla $\phi_i(\alpha_1) = \alpha_i$ ja $\phi_i|_K = \mathrm{id}_K$.

Kunta L on polynomin $f(x)$ juurikunta sekä kunnan $K(\alpha_1)$ että kunnan $K(\alpha_i)$ suhteen, joten lauseen 4.6 perusteella kukin isomorfismi ϕ_i voidaan jatkaa isomorfismiksi $\Phi_i \colon L \to L$, jolla $\Phi_i|_{K(\alpha_1)} = \phi_i$. Tällöin kukin Φ_i on siis K-automorfismi kunnassa L, joten $\Phi_i \in \mathrm{Gal}(L/K)$ ja lisäksi $\Phi_i(\alpha_1) = \phi_i(\alpha_1) = \alpha_i$ kaikilla i.

Osoitetaan laajennuksen L/K olevan Galois näyttämällä, että $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$. Ryhmä $\mathrm{Gal}(L/K)$ koostuu K-automorfismeista, joten kunta K sisältyy joka tapauksessa kiintokuntaan $\mathrm{Fix}(\mathrm{Gal}(L/K))$. Riittää siis osoittaa $\mathrm{Fix}(\mathrm{Gal}(L/K)) \subset K$. Oletetaan siis, että $\beta \in \mathrm{Fix}(\mathrm{Gal}(L/K))$, ja osoitetaan, että tällöin $\beta \in K$. Jokainen $K(\alpha)$-automorfismi kiinnittää myös kunnan K, joten $\mathrm{Fix}(\mathrm{Gal}(L/K)) \subset \mathrm{Fix}(\mathrm{Gal}(L/K(\alpha_1))) = K(\alpha_1)$ ja siten $\beta \in K(\alpha_1)$. Lauseen 2.14 perusteella alkio β voidaan siis esittää muodossa

$$\beta = k_{s-1}\alpha_1^{s-1} + \cdots + k_1\alpha_1 + k_0,$$

missä $k_i \in K$. Alkio β oletettiin K-automorfismien kiintokunnan alkioksi, joten K-automorfismi Φ_i pitää sen paikallaan. Näin siis $\Phi_i(\beta) = \beta$ ja kuitenkin

$$\Phi_i(\beta) = k_{s-1}\alpha_i^{s-1} + \cdots + k_1\alpha_i + k_0.$$

Tarkastellaan nyt polynomia

$$p(x) = k_{s-1}x^{s-1} + \cdots + k_1x + (k_0 - \beta).$$

Tiedetään, että $\beta = \Phi_i(\beta)$, joten sijoittamalla α_i polynomiin $p(x)$ saadaan

$$\begin{aligned} p(\alpha_i) &= k_{s-1}\alpha_i^{s-1} + \cdots + k_1\alpha_i + (k_0 - \beta) \\ &= k_{s-1}\alpha_i^{s-1} + \cdots + k_1\alpha_i + k_0 - \Phi_i(\beta) \\ &= k_{s-1}\alpha_i^{s-1} + \cdots + k_1\alpha_i + k_0 - (k_{s-1}\alpha_i^{s-1} + \cdots + k_1\alpha_i + k_0) \\ &= 0. \end{aligned}$$

Polynomilla $p(x)$ on siis s juurta $\alpha_1, \alpha_2, \ldots, \alpha_s$, jotka ovat toisistaan erillisiä, sillä ne ovat myös polynomin $f(x)$ juuria, ja polynomi $f(x)$ oletettiin separoituvaksi. Polynomin $p(x)$ aste on kuitenkin vain $s - 1$, ja koska nollasta poikkeavalla polynomilla voi olla korkeintaan asteensa verran juuria, on polynomin $p(x)$ oltava nollapolynomi. Polynomin $p(x)$ jokainen vakiokerroin on siis nolla, joten myös $k_0 - \beta = 0$, mistä seuraa $\beta \in K$. Siis $\mathrm{Fix}(\mathrm{Gal}(L/K)) = K$. □

Esimerkki 6.5. Esimerkissä 3.6 osoitettiin, että laajennus $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ on separoituvan polynomin $f(x) = x^4 - 5x + 6 = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ juurikunta. Laajennus on siis sekä Galois että normaali ja separoituva.

Laajennuksen $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ olisi voinut osoittaa separoituvaksi myös käyttämällä suoraan lausetta 3.11. Kunnan $\mathbb{Q}$ karakteristika on nolla, joten mikä tahansa rationaalikertoiminen polynomi on separoituva, mistä seuraa myös, että minkä tahansa kunnan $\mathbb{Q}$ laajennuksen alkion minimipolynomi on separoituva. Mutta vaikka laajennuksen separoituvuus saataisinkiin suoraan lähtökunnan karakteristikasta, laajennuksen näyttäminen normaaliksi tai Galois'n laajennukseksi ei yleensä onnistuisi läheskään yhtä helposti ilman lausetta 6.4.

6.2 Galois'n teorian peruslause

Galois'n teorian peruslauseen todistaminen vaatii vielä kiintokuntiin liittyvän aputuloksen, joka on luonteeltaan varsin tekninen. Lemma käsittelee aliryhmien konjugaatteja, joten ei ole yllättävää, että lemmaa käytetään jatkossa nimenomaan normaalien aliryhmien yhteydessä.

Lemma 6.6. *Olkoon G ryhmä K-automorfismeja kunnassa L ja olkoon $H \leq G$. Oletetaan, että $M = \mathrm{Fix}(H)$. Tällöin $\sigma(M) = \mathrm{Fix}(\sigma H \sigma^{-1})$ kaikilla $\sigma \in G$.*

Todistus. Olkoon $\sigma \in G$. Osoitetaan ensin, että $\sigma(M) \subset \mathrm{Fix}(\sigma H \sigma^{-1})$. Oletetaan, että $\sigma(m) \in \sigma(M)$ jollain $m \in M$, ja olkoon $\tau \in H$. Kuvaus τ kiinnittää alkion $m \in M$, joten

$$\sigma\tau\sigma^{-1}(\sigma(m)) = \sigma\tau(m) = \sigma(m).$$

Näin ollen $\sigma(m) \in \mathrm{Fix}(\sigma H \sigma^{-1})$, joten $\sigma(M) \subset \mathrm{Fix}(\sigma H \sigma^{-1})$.

Kääntäen, oletetaan, että $m' \in \mathrm{Fix}(\sigma H \sigma^{-1})$. Tällöin siis $\sigma\tau\sigma^{-1}(m') = m'$ kaikilla kuvauksilla $\tau \in H$, joten ryhmän laskusääntöjä käyttämällä saadaan $\tau\sigma^{-1}(m') = \sigma^{-1}(m')$. Valitaan $m = \sigma^{-1}(m')$. Osoitetaan, että tällöin $m \in M$, jolloin siis pätisi $m' \in \sigma(M)$. Nyt

$$\tau(m) = \tau\sigma^{-1}(m') = \sigma^{-1}(m') = m,$$

joten $m \in \mathrm{Fix}(H) = M$. Siis $m' \in \sigma(M)$ ja edelleen $\mathrm{Fix}(\sigma H \sigma^{-1}) \subset \sigma(M)$. □

Nyt olemmekin valmiit todistamaan Galois'n teorian peruslauseen. Kolmiosaisen lauseen ensimmäinen osa määrittelee niin kutsutun Galois'n yhteyden, ja muut kaksi osaa syventävät tietojamme siitä. Peruslause osoittaa myös, että jokainen sopivasti valittu Galois'n laajennuksen välilaajennus on itsekin Galois.

Lause 6.7. (Galois'n teorian peruslause.) *Olkoon L kunnan K äärellinen Galois'n laajennus ja olkoon $G = \mathrm{Gal}(L/K)$. Tällöin pätevät seuraavat väitteet:*

1. *Laajennuksen L/K välikuntien $K \subset M \subset L$ ja ryhmän G aliryhmien $G \geq H \geq \{1\}$ välillä on yksi–yhteen-vastaavuus, jonka antavat kuvaukset $M \mapsto \mathrm{Gal}(L/M)$ ja $H \mapsto \mathrm{Fix}(H)$.*

2. *Olkoot $H \leq G$ ja $M = \mathrm{Fix}(H)$. Tällöin $H \trianglelefteq G$, jos ja vain jos M/K on Galois'n laajennus. Lisäksi pätee, että jos $H \trianglelefteq G$, niin $\mathrm{Gal}(M/K) \cong G/H$.*

3. *Kaikille välilaajennuksille $K \subset M \subset L$ pätee $[L : M] = |\mathrm{Gal}(L/M)|$ ja $[M : K] = [G : \mathrm{Gal}(L/M)]$.*

Todistus. 1. Merkitään $\Gamma\colon M \mapsto \mathrm{Gal}(L/M)$ ja $\Psi\colon H \mapsto \mathrm{Fix}(H)$. Osoitetaan väite näyttämällä, että $\Gamma \circ \Psi = \mathrm{id}$ ja $\Psi \circ \Gamma = \mathrm{id}$.

Olkoon M laajennuksen L/K välikunta. Laajennus L/K on Galois, joten lauseen 6.4 nojalla L on jonkin separoituvan K-kertoimisen polynomin $f(x)$ juurikunta. Kuitenkin pätee $K \subset M$, joten $f(x) \in M[x]$. Kunta L on siis separoituvan M-kertoimisen polynomin juurikunta, joten myös laajennus L/M on Galois. Näin ollen $\mathrm{Fix}(\mathrm{Gal}(L/M)) = M$, joten

$$\Psi(\Gamma(M)) = \Psi(\mathrm{Gal}(L/M)) = \mathrm{Fix}(\mathrm{Gal}(L/M)) = M.$$

Kääntäen, olkoon $H \leq G$. Merkitään $F = \mathrm{Fix}(H)$. Aliryhmä H on äärellinen ryhmä kunnan L eri automorfismeja, joten lauseen 5.12 nojalla $H = \mathrm{Gal}(L/F)$, mistä seuraa, että

$$\Gamma(\Psi(H)) = \Gamma(\mathrm{Fix}(H)) = \Gamma(F) = \mathrm{Gal}(L/F) = H.$$

Kuvaukset Γ ja Ψ ovat siis toistensa käänteiskuvauksia, joten niiden määrittelemä yhteys aliryhmien H ja välikuntien M välillä on bijektiivinen.

2. Oletetaan, että H on ryhmän $\mathrm{Gal}(L/K)$ normaali aliryhmä. Osoitetaan, että laajennus M/K on tällöin normaali ja separoituva. Olkoon $f(x) \in K[x]$ jaoton polynomi, ja oletetaan, että sillä on juuri a kunnassa M. Olkoon nyt b jokin toinen polynomin $f(x)$ juuri. Tällöin isomorfismien jatkamislauseen 4.6 perusteella on olemassa jokin $\sigma \in \mathrm{Gal}(L/K)$, jolla $\sigma(a) = b$. Kuvaukseen σ voidaan nyt soveltaa yleistä ryhmien teoriaa, jonka mukaan kaikilla $\tau \in H$ pätee $\tau(b) = \tau(\sigma(a)) = \sigma(\sigma^{-1}\tau\sigma(a))$. Aiemmin kuitenkin oletettiin $H \trianglelefteq G$, minkä vuoksi $\sigma^{-1}\tau\sigma \in H$. Alkion a puolestaan oletettiin kuuluvan aliryhmän H kiintokuntaan, joten $\sigma^{-1}\tau\sigma(a) = a$. Näin ollen

$$\tau(b) = \sigma(\sigma^{-1}\tau\sigma(a)) = \sigma(a) = b,$$

eli toisin sanottuna $b \in \mathrm{Fix}(H) = M$. Kaikki polynomin $f(x)$ juuret ovat siis kunnassa M, joten laajennus M/K on normaali.

Osoitetaan vielä, että laajennus M/K on separoituva. Olkoon $m(x) \in K[x]$ jonkin alkion $a \in M$ minimipolynomi. Laajennus L/K on Galois, joten lauseen 6.4 perusteella se on separoituva. Kunnan L alkioiden minimipolynomit kunnan K suhteen ovat siis separoituvia, joten koska $a \in M \subset L$, on myös alkion a minimipolynomin $m(x)$ oltava separoituva. Laajennus M/K on siis separoituva, ja koska aiemmin se näytettiin myös normaaliksi, niin lauseen 6.4 perusteella laajennus M/K on Galois.

Osoitetaan vielä, että jos $H \trianglelefteq G$, niin $\mathrm{Gal}(M/K) \cong G/H$. Määritellään rajoittumakuvaus

$$\mu\colon G \to \mathrm{Gal}(M/K), \qquad \mu(\sigma) = \sigma|_M.$$

Koska H on normaali aliryhmä, niin kaikilla $\sigma \in G$ saadaan lemman 6.6 avulla

$$\sigma(M) = \mathrm{Fix}(\sigma H \sigma^{-1}) = \mathrm{Fix}(H) = M,$$

joten kuvauksen μ maalijoukko $\mathrm{Im}(\mu)$ tosiaankin on $\mathrm{Gal}(M/K)$. On myös suoraviivaista osoittaa, että kuvaus μ on homomorfismi, jonka ydin $\mathrm{Ker}(\mu) = \{\sigma \in G : \sigma|_M = \mathrm{id}_M\}$ on $\mathrm{Gal}(L/M)$. Nyt ryhmien homomorfialauseen perusteella pätee

$$\mathrm{Im}(\mu) \cong G/\mathrm{Ker}(\mu),$$

eli toisin sanottuna

$$\mathrm{Gal}(M/K) \cong G/\mathrm{Gal}(L/M).$$

Lauseen 5.12 perusteella pätee kuitenkin $\mathrm{Gal}(L/M) = H$, joten $\mathrm{Gal}(M/K) \cong G/H$.

Kääntäen, oletetaan, että laajennus M/K on Galois. Tällöin M on jonkin separoituvan polynomin $f(x) \in K[x]$ juurikunta lauseen 6.4 perusteella. Olkoot $\alpha_1, \ldots, \alpha_m \in M$ polynomin $f(x)$ juuret, jolloin juurikunnan määritelmästä saadaan $M = K(\alpha_1, \ldots, \alpha_m)$.

Olkoon $\sigma \in \mathrm{Gal}(L/K)$. Koska $f(x) \in K[x]$, niin kuvaus σ permutoi sen juuria lauseen 5.2 nojalla, eli kaikilla i pätee $\sigma(\alpha_i) = \alpha_j$ jollakin j. Lisäksi $\sigma(M) = M$, sillä kukin kunnan M alkio voidaan esittää tuloksen 3.5 nojalla lineaarikombinaationa juurista α_i ja kuvaus σ permutoi juuria α_i ja pitää lineaarikombinaation kertoimet $k_i \in K$ paikallaan. Nyt siis lemmaan 6.6 nojaten $\mathrm{Fix}(H) = M = \sigma(M) = \mathrm{Fix}(\sigma H \sigma^{-1})$. On siis löydetty kaksi ryhmän G aliryhmää H ja $\sigma H \sigma^{-1}$, joilla on sama kiintokunta M. Peruslauseen kohdan 1 mukaan Galois'n ryhmän G aliryhmien ja laajennuksen L/K välikuntien välillä on yksi–yhteenvastaavuus, joten jos kahdella aliryhmällä on sama kiintokunta, ovat aliryhmät samat. On siis oltava $H = \sigma H \sigma^{-1}$, joten H on ryhmän G normaali aliryhmä.

3. Laajennus L/K on Galois, joten voidaan soveltaa vastaavaa päättelyä kuin kohdan 1 todistuksen alussa. Kunta L on jonkin separoituva polynomin $f(x) \in K[x]$ juurikunta lauseen 6.4 nojalla, mutta koska $K \subset M$, niin kunta L on separoituvan polynomin $f(x) \in M[x]$ juurikunta. Näin ollen laajennus L/M on lauseen 6.4 nojalla Galois, joten $\mathrm{Fix}(\mathrm{Gal}(L/M)) = M$. Nyt lauseesta 5.12 saadaan $[L : M] = |\mathrm{Gal}(L/M)|$.

Osoitetaan vielä, että $[M : K] = [G : \mathrm{Gal}(L/M)]$. Lauseesta 2.5 saadaan

$$[M : K] = \frac{[L : K]}{[L : M]},$$

ja toisaalta Lagrangen lauseen perusteella

$$|\mathrm{Gal}(L/M)| = \frac{|G|}{[G : \mathrm{Gal}(L/M)]},$$

joten

$$[M : K] = \frac{[L : K]}{[L : M]} = \frac{[L : K]}{|G|} \cdot [G : \mathrm{Gal}(L/M)].$$

Laajennus L/K on kuitenkin Galois, joten lauseen 5.12 perusteella $[L : K] = |G|$ eli lopulta

$$[M : K] = \frac{[L : K]}{|G|} \cdot [G : \mathrm{Gal}(L/M)] = [G : \mathrm{Gal}(L/M)].$$

□

Luvun päättävä esimerkki yhdistelee peruslauseen lisäksi monia muita aiemmin käsiteltyjä asioita. Galois'n ryhmän määrittämisen lisäksi esimerkissä poraudutaan Galois'n

ryhmän aliryhmän kiintokuntaan ja tutkitaan, miten aliryhmän kuvaus käsittelee laajennuskunnan alkioita. Tarkasteltavan polynomi on lisäksi separoituva, joten Galois'n ryhmään saadaan kaikki mahdolliset juurten permutaatiot.

Esimerkissä käsiteltävä Galois'n ryhmän aliryhmän kiintokunnan määrittäminen sisältää myös kaikuja Galois'n alkuperäisestä lähestymistavasta, jossa tutkittiin, millaiset juurten permutaatiot säilyttävät niiden väliset suhteet. Galois'n lähestymistapaa esitellään esimerkiksi teoksessa [10], s. 238.

Esimerkki 6.8. Tutkitaan polynomin $f(x) = x^4 - 3 \in \mathbb{Q}[x]$ Galois'n ryhmää. Polynomin $f(x)$ juuret ovat $\pm\sqrt[4]{3}$ ja $\pm i\sqrt[4]{3}$, joten sen juurikunta on $L = \mathbb{Q}(\sqrt[4]{3}, i)$ (esimerkki 3.6 käsittelee juurikunnan määrittämistä tarkemmin). Kunnan $\mathbb{Q}$ karakteristika on nolla, joten lauseen 3.11 nojalla polynomi $f(x)$ on separoituva. Siispä lauseen 6.4 nojalla laajennus $L/\mathbb{Q}$ on separoituvan $\mathbb{Q}$-kertoimisen polynomin juurikuntana Galois, joten peruslausetta 6.7 voidaan soveltaa.

Määritetään ensin polynomin $f(x)$ Galois'n ryhmän koko. Laajennuksen $L/\mathbb{Q}$ aste voidaan lauseen 2.5 mukaisesti pilkkoa muotoon

$$[L : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}(\sqrt[4]{3})][\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}].$$

Polynomi $f(x)$ on jaoton renkaassa $\mathbb{Q}[x]$ Eisensteinin kriteerin perusteella, joten $f(x)$ on alkion $\sqrt[4]{3}$ minimipolynomi, ja siten $[\mathbb{Q}(\sqrt[4]{3}) : \mathbb{Q}] = 4$. Alkion i minimipolynomi kunnan $\mathbb{Q}(\sqrt[4]{3})$ suhteen on $x^2 + 1$, sillä i on sen juuri ja kuitenkin $i \notin \mathbb{Q}(\sqrt[4]{3}) \subset \mathbb{R}$. Näin ollen $[\mathbb{Q}(\sqrt[4]{3}, i) : \mathbb{Q}(\sqrt[4]{3})] = 2$, joten $[L : \mathbb{Q}] = 2 \cdot 4 = 8$. Lauseen 5.12 perusteella siis tiedetään, että polynomin $f(x)$ Galois'n ryhmässä on kahdeksan alkiota.

Isomorfismien jatkamislauseen 4.6 nojalla juurikunnassa $L/\mathbb{Q}$ on olemassa jokin $\mathbb{Q}$-automorfismi σ, jolla $\sigma(\sqrt[4]{3}) = i\sqrt[4]{3}$ ja $\sigma(i) = i$ (laajennettava isomorfismi on kunnan $\mathbb{Q}(i)$ identtinen kuvaus itselleen). Samoin on olemassa $\mathbb{Q}$-automorfismi τ, jolla $\tau(\sqrt[4]{3}) = \sqrt[4]{3}$ ja $\tau(i) = -i$. Yhdessä automorfismit σ ja τ generoivat seuraavat kahdeksan erillistä juurikunnan $\mathbb{Q}$-automorfismia, jotka muodostavat polynomin $f(x)$ Galois'n ryhmän:

$$\epsilon = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \end{pmatrix} \qquad \sigma = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ i\sqrt[4]{3} & -i\sqrt[4]{3} & -\sqrt[4]{3} & \sqrt[4]{3} \end{pmatrix}$$

$$\sigma^2 = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ -\sqrt[4]{3} & \sqrt[4]{3} & -i\sqrt[4]{3} & i\sqrt[4]{3} \end{pmatrix} \qquad \sigma^3 = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ -i\sqrt[4]{3} & i\sqrt[4]{3} & \sqrt[4]{3} & -\sqrt[4]{3} \end{pmatrix}$$

$$\tau = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ \sqrt[4]{3} & -\sqrt[4]{3} & -i\sqrt[4]{3} & i\sqrt[4]{3} \end{pmatrix} \qquad \sigma\tau = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ i\sqrt[4]{3} & -i\sqrt[4]{3} & \sqrt[4]{3} & -\sqrt[4]{3} \end{pmatrix}$$

$$\sigma^2\tau = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ -\sqrt[4]{3} & \sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \end{pmatrix} \qquad \sigma^3\tau = \begin{pmatrix} \sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} \\ -i\sqrt[4]{3} & i\sqrt[4]{3} & -\sqrt[4]{3} & \sqrt[4]{3} \end{pmatrix}$$

Mekaanisesti laskemalla voidaan myös määrittää Galois'n ryhmän aliryhmät:

Yksi alkio:	$\{\epsilon\}$
Kaksi alkiota:	$\{\epsilon, \sigma^2\},\ \{\epsilon, \tau\},\ \{\epsilon, \sigma\tau\},\ \{\epsilon, \sigma^2\tau\},\ \{\epsilon, \sigma^3\tau\}$
Neljä alkiota:	$\{\epsilon, \sigma, \sigma^2, \sigma^3\},\ \{\epsilon, \sigma^2, \tau, \sigma^2\tau\},\ \{\epsilon, \sigma^2, \sigma\tau, \sigma^3\tau\}$
Kahdeksan alkiota:	$\{\epsilon, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$

Merkitään $G = \mathrm{Gal}(L/\mathbb{Q}) = \{\epsilon, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$. Tutkitaan nyt millaista tietoa Galois'n teorian peruslause 6.7 antaa laajennuksesta $L/\mathbb{Q}$. Lauseen ensimmäisen kohdan mukaan kutakin aliryhmää $H \leq G$ vastaa Galois'n laajennuksen välikunta $\mathrm{Fix}(H)$. Määritellään vaikkapa aliryhmän $H = \{\epsilon, \sigma^3\tau\}$ kiintokunta. Esimerkkiä 3.6 mukaillen välilaajennuksen $\mathbb{Q}(\sqrt[4]{3})$ alkiot voidaan esittää muodossa

$$q_0 + q_1\sqrt[4]{3} + q_2(\sqrt[4]{3})^2 + q_3(\sqrt[4]{3})^3,$$

missä $q_i \in \mathbb{Q}$. Vastaavasti päättelemällä juurikunnan $\mathbb{Q}(\sqrt[4]{3}, i)$ alkiot voidaan esittää muodossa

$$\begin{aligned} &(q_0 + q_1\sqrt[4]{3} + q_2(\sqrt[4]{3})^2 + q_3(\sqrt[4]{3})^3) + (r_0 + r_1\sqrt[4]{3} + r_2(\sqrt[4]{3})^2 + r_3(\sqrt[4]{3})^3)i \\ &= q_0 + q_1\sqrt[4]{3} + q_2(\sqrt[4]{3})^2 + q_3(\sqrt[4]{3})^3 + r_0 i + r_1 i\sqrt[4]{3} + r_2 i(\sqrt[4]{3})^2 + r_3 i(\sqrt[4]{3})^3, \end{aligned} \tag{6.9}$$

missä $q_i, r_i \in \mathbb{Q}$.

Olkoon $\alpha \in \mathrm{Fix}(H)$. Soveltamalla kuvauksen $\sigma^3\tau$ määritelmää kuhunkin lausekkeen (6.9) termiin ja järjestämällä sitten lopputulos samaisen lausekkeen (6.9) mukaiseksi saadaan

$$\begin{aligned}\sigma^3\tau(\alpha) &= q_0 - q_1 i\sqrt[4]{3} - q_2(\sqrt[4]{3})^2 + q_3 i(\sqrt[4]{3})^3 - r_0 i - r_1\sqrt[4]{3} + r_2 i(\sqrt[4]{3})^2 + r_3(\sqrt[4]{3})^3 \\ &= q_0 - r_1\sqrt[4]{3} - q_2(\sqrt[4]{3})^2 + r_3(\sqrt[4]{3})^3 - r_0 i - q_1 i\sqrt[4]{3} + r_2 i(\sqrt[4]{3})^2 + q_3 i(\sqrt[4]{3})^3. \qquad (6.10)\end{aligned}$$

Kuvaus $\sigma^3\tau$ pitää kiintokunnan alkion α paikallaan, joten vertailemalla saatua lauseketta (6.10) aiempaan lausekkeeseen (6.9) voidaan päätellä, että

$$r_1 = -q_1, \quad q_2 = -q_2 = 0, \quad r_3 = q_3 \quad \text{ja} \quad r_0 = -r_0 = 0.$$

Lauseke (6.10) voidaan siis sieventää muotoon

$$\begin{aligned}\sigma^3\tau(\alpha) &= q_0 + q_1\sqrt[4]{3} + q_3(\sqrt[4]{3})^3 - q_1 i\sqrt[4]{3}i + r_2 i(\sqrt[4]{3})^2 + q_3 i(\sqrt[4]{3})^3 \\ &= q_0 + q_1(1-i)\sqrt[4]{3} + r_2 i(\sqrt[4]{3})^2 + q_3(1+i)(\sqrt[4]{3})^3 \\ &= q_0 + q_1(1-i)\sqrt[4]{3} - \frac{r_2}{2}(-2i)(\sqrt[4]{3})^2 - \frac{q_3}{2}(-2-2i)(\sqrt[4]{3})^3 \\ &= q_0 + q_1\left((1-i)\sqrt[4]{3}\right) - \frac{r_2}{2}\left((1-i)\sqrt[4]{3}\right)^2 - \frac{q_3}{2}\left((1-i)\sqrt[4]{3}\right)^3. \qquad (6.11)\end{aligned}$$

Tulkitsemalla lopuksi lauseketta (6.11) lauseen 2.14 valossa nähdään, että alkio α on laajennuksen $\mathbb{Q}((1-i)\sqrt[4]{3})/\mathbb{Q}$ alkio. Aliryhmän H kiintokunta on siis $M = \mathbb{Q}((1-i)\sqrt[4]{3})$.

Aliryhmä H ei kuitenkaan ole ryhmän G normaali aliryhmä, sillä $\sigma \in G$ ja kuitenkin

$$\sigma(\sigma^3\tau)\sigma^{-1} = \sigma^4\tau\sigma^{-1} = \epsilon\tau\sigma^{-1} = \tau^{-1}\sigma^{-1} = (\sigma\tau)^{-1} = \sigma\tau \notin H.$$

Nyt peruslauseen toisesta osasta seuraakin suoraan, että $M/\mathbb{Q}$ ei ole Galois'n laajennus.

Aliryhmään H voidaan kuitenkin soveltaa lausetta 5.12, jolloin saadaan esitysmuoto $H = \mathrm{Gal}(L/M)$. Peruslauseen kolmas osa kertookin nyt, että

$$[L : M] = |\mathrm{Gal}(L/M)| = |H| = 2$$

ja lisäksi

$$[M : \mathbb{Q}] = [G : \mathrm{Gal}(L/M)] = \frac{|G|}{|\mathrm{Gal}(L/M)|} = \frac{|G|}{|H|} = \frac{8}{2} = 4.$$

Luku 7

Kuntien laajentaminen juurtamalla

Edellisen luvun päättäneessä esimerkissä 6.8 huomattiin, että polynomin Galois'n ryhmän määrittäminen on varsin työlästä. Galois'n ryhmä lukuisine aliryhmineen ei myöskään onnistunut paljastamaan mitään tutkitun polynomin juurtamalla ratkeavuudesta. Tässä luvussa tutkitaan, voidaanko juurtamalla ratkeavuus selvittää suoraan Galois'n ryhmän sisäisestä rakenteesta määrittämättä koskaan itse Galois'n ryhmää.

Tätä tarkoitusta varten määritellään ensin juurtamalla ratkeavuus kuntalaajennusten näkökulmasta tutkimalla niin kutsuttuja juurilaajennuksia. Galois'n teorian peruslause yhdistää juurilaajennuksen jokaiseen välilaajennukseen tietynlaisen Galois'n ryhmän aliryhmän, jolloin Galois'n ryhmän sisäiseen rakenne alkaa hahmottua. Tavoitteenamme on nähdä, onko juurtamalla ratkeavan polynomin Galois'n ryhmässä *aina* löydettävissä jokin tietty rakenne, joka olisi tällöin välttämätön ehto juurtamalla ratkeavuudelle.

7.1 Juurilaajennukset

Aloitetaan juurtamalla ratkeavuuden tutkiminen määrittelemällä juurilaajennukset.

Määritelmä 7.1. Kunta J on kunnan K *juurilaajennus*, jos on olemassa jono kuntia

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = J,$$

missä $K_{i+1} = K_i(\alpha_i)$ jollain sellaisella $\alpha_i \in K_{i+1}$, että $\alpha_i^{n_i} \in K_i$ jollain $n_i \in \mathbb{N}$. Laajennuksen sanotaan olevan *n-juurilaajennus*, jos $n_1 = \cdots = n_m = n$.

Mikä tahansa juurilaajennus on n-juurilaajennus, kun valitaan $n = n_1 n_2 \cdots n_m$. Yksinkertaisuuden vuoksi tästä eteenpäin keskitytäänkin n-juurilaajennuksiin, ellei toisin mainita.

Nimi *juuri*laajennus (engl. *radical extension*) ei niinkään viittaa polynomin juuriin, vaan juurroksiin. Määritelmän 7.1 mukainen n-juurilaajennus J voitaisiinkin esittää muodossa

$$J = K(\sqrt[n]{\alpha_0}, \sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_{n-1}}).$$

Juurilaajennukselle olennainen välilaajennusten torni syntyykin juuren ottamisen taipumuksesta tuottaa alkioita kunnan ulkopuolelta. Jos nimittäin alkiolle $k \in K$ pätee $\alpha^n = k$ jollain alkiolla α, ei ole mitään takeita siitä, että myös alkio α olisi kunnan K alkio. Lisäämällä kuntaan K sen ulkopuolinen juurros α saadaan siis laajennus $K(\alpha)$, joka on varmasti äärellinen, sillä sen minimipolynomin aste on korkeintaan n. Samoin voidaan menetellä myös kunnalle $K(\alpha)$, ja näin jatkaen voidaan luoda monitasoisia, mutta silti rakenteeltaan hallittuja kuntalaajennusten torneja.

Esimerkki 7.2. Pyritään löytämään kunnan $\mathbb{Q}$ laajennus, joka sisältäisi luvun

$$\lambda = \sqrt{\frac{3 + \sqrt[3]{2}}{\sqrt[7]{3 + \sqrt{3}}}} \in \mathbb{R}.$$

Luvun λ kaltaisen monimutkaisen juurroksen käsitteleminen onnistuu helpoiten pilkkomalla se pienempiin osiin juurros kerrallaan. Olkoot

$$\alpha^2 = 3, \qquad \beta^7 = 3 + \alpha, \qquad \gamma^3 = 2 \quad \text{ja} \quad \delta^2 = \frac{3 + \gamma}{\beta}.$$

Näin määriteltynä laajennus $\mathbb{Q}(\alpha, \beta, \gamma, \delta)$ on juurilaajennus, sillä

$$\alpha^2 \in \mathbb{Q}, \quad \beta^7 \in \mathbb{Q}(\alpha), \quad \gamma^3 \in \mathbb{Q}(\alpha, \beta) \quad \text{ja} \quad \delta^2 \in Q(\alpha, \beta, \gamma).$$

Lisäksi $\lambda = \delta \in \mathbb{Q}(\alpha, \beta, \gamma, \delta)$.

Rationaalikertoimisten polynomien juuret ovat usein rationaalilukujen juurroksia, jotka ovat kunnan $\mathbb{Q}$ ulkopuolella. Osoittautuukin, että sopivan juurilaajennuksen löytyminen on täysin sama asia kuin juurtamalla ratkeavuus.

Määritelmä 7.3. Polynomi $f(x) \in K[x]$ on *juurtamalla ratkeava*, jos on olemassa juurilaajennus L/K, missä $f(x)$ jakautuu ensimmäisen asteen tekijöihin.

Yllä oleva määritelmä juurtamalla ratkeavuudelle vaikuttaa ensi näkemältä varsin erilaiselta kuin johdantoluvussa annettu määritelmä 1.1. Vaatimus polynomin jakautumisesta ensimmäisen asteen tekijöihin tarkoittaa, että laajennus sisältää polynomin kaikki juuret, minkä voi nähdä eräänlaisena minimivaatimuksena polynomin ratkeavuudesta puhumiselle. Itse juurilaajennuksen yhteys määritelmään 1.1 ei kuitenkaan ole aivan yhtä suoraviivainen, mutta seuraava esimerkki havainnollistaa tilannetta.

Esimerkki 7.4. Tarkastellaan yleistä toisen asteen polynomia $f(x) = ax^2+bx+c \in \mathbb{Q}[x]$. Jos alkiot $\alpha_1, \alpha_2 \in \mathbb{C}$ ovat polynomin $f(x)$ juuret, niin toisen asteen yhtälön ratkaisukaavan perusteella pätee

$$\alpha_i = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

joillakin $a, b, c \in \mathbb{Q}$. Polynomin $f(x)$ molemmat juuret ovat siis ilmaistavissa rationaalilausekkeina kunnan $\mathbb{Q}$ alkioista ja niiden juurista, joten polynomi $f(x)$ on juurtamalla ratkeava johdantoluvun määritelmän 1.1 mukaan.

Kummallekin juurelle kuitenkin pätee

$$\alpha_i = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} = -\frac{b}{2a} \pm \frac{1}{2a}\sqrt{b^2 - 4ac},$$

joten lauseen 2.14 perusteella alkio α_i on laajennuksen $\mathbb{Q}(\sqrt{b^2 - 4ac})$ alkio. Koska kuitenkin $(\sqrt{b^2 - 4ac})^2 \in \mathbb{Q}$, niin laajennus $\mathbb{Q}(\sqrt{b^2 - 4ac})/\mathbb{Q}$ on juurilaajennus, joten polynomi $f(x)$ on juurtamalla ratkeava myös yllä olevan määritelmän 7.3 mukaisesti.

7.2 Ykkösenjuuret

Juurtamalla ratkeavalla polynomilla on aina olemassa jokin juurilaajennus, joka koostuu sisäkkäisten kuntalaajennusten tornista. Pyritään nyt soveltamaan Galois'n teorian peruslausetta 6.7 juurilaajennuksen ja erityisesti sen välilaajennusten tutkimiseen.

Peruslauseen soveltaminen vaatii kuitenkin sovelluskohteena olevan laajennuksen olevan Galois, joten otetaan nyt käyttöön apuneuvot, joiden avulla juurilaajennuksen kustakin välilaajennuksesta saadaan Galois'n laajennus. Keskeisimmäksi näistä apuneuvoista nousevat ykkösenjuuret ja ennen kaikkea primitiivinen ykkösenjuuri.

Määritelmä 7.5. Jos $\omega^n = 1$ jollain $\omega \in K$, niin alkion ω sanotaan olevan *n:s ykkösenjuuri*. Ykkösenjuuren sanotaan olevan *primitiivinen*, jos lisäksi $\omega^m \neq 1$ kaikilla $1 \leq m < n$.

Voidaan osoittaa, että n:net ykkösenjuuret muodostavat kertolaskuryhmän. Kukin ryhmän alkio on polynomin $f(x) = x^n - 1$ juuri, joten ykkösenjuurten ryhmässä on korkeintaan n alkiota. Jos kunnan karakteristika on kuitenkin nolla, on polynomi $f(x)$ separoituva, jolloin erillisiä ykkösenjuuria on tasan n kappaletta. Jos karakteristika on nolla, niin se itse asiassa myös mahdollistaa primitiivisen n:nen ykkösenjuuren olemassaolon, kuten seuraava lause osoittaa.

Lause 7.6. *Oletetaan, että K on kunta, jonka karakteristika on nolla. Tällöin kunnalla K on olemassa primitiivinen n:s ykkösenjuuri jossain kunnan K laajennuksessa.*

Todistus. Tarkastellaan polynomia $f(x) = x^n - 1 \in K[x]$. Olkoon L polynomin $f(x)$ juurikunta. Kunnan K karakteristika on nolla, joten lauseen 3.11 nojalla polynomin $f(x)$ kaikki n juurta ovat erillisiä kunnan L alkioita. Jokainen polynomin $f(x)$ juuri on kuitenkin ykkösenjuuri, ja kuten ykkösenjuurten määritelmän yhteydessä todettiin, ykkösenjuuret muodostavat kertolaskuryhmän L^* aliryhmän. Tämän aliryhmän kertaluku on n, mutta mikä tahansa kunnan kertolaskuryhmän äärellinen aliryhmä on syklinen, mikä on todistettu esimerkiksi teoksessa [12], s. 12. Ykkösenjuurten ryhmällä on siis jokin virittäjäalkio $\omega \in L$.

Osoitetaan vielä, että n:s ykkösenjuuri ω on primitiivinen. Oletetaan, että näin ei olisi, jolloin siis olisi olemassa jokin $1 \leq m < n$, jolla $\omega^m = 1$. Tällöin alkion ω virittämän ryhmän koko olisikin siis $m < n$, mikä on ristiriita. Kunnalla K on siis olemassa primitiivinen n:s ykkösenjuuri $\omega \in L$. □

Primitiivinen n:s ykkösenjuuri ω virittää siis kaikkien n:nsien ykkösenjuurten ryhmän $\{1, \omega, \omega^2, \ldots, \omega^{n-1}\}$. Kukin ryhmän jäsen tosiaankin on n:s ykkösenjuuri, sillä mille tahansa ω^r pätee

$$(\omega^r)^n = \omega^{rn} = (\omega^n)^r = 1^r = 1.$$

Galois'n yhteyden soveltamisen mahdollistava primitiivinen n:s ykkösenjuuri ω on siis löydettävissä jostain kunnan *laajennuksesta*, jos kunnan karakteristika on nolla. Primitiivinen n:s ykkösenjuuri ei siis sisälly mielivaltaiseen kerroinkuntaan, joten kerroinkunnan laajentaminen on syytä aloittaa alkiosta ω.

Lause 7.7. *Olkoon K kunta, jonka karakteristika on nolla, ja olkoon ω primitiivinen n:s ykkösenjuuri. Tällöin laajennus $K(\omega)/K$ on Galois ja sen Galois'n ryhmä on vaihdannainen.*

Todistus. Osoitetaan, että laajennus $K(\omega)$ on polynomin $f(x) = x^n - 1$ juurikunta, jotta voidaan käyttää lausetta 6.4. Polynomin $f(x)$ juuret ovat kaikki n:net ykkösenjuuret, ja koska primitiivinen ykkösenjuuri ω virittää ykkösenjuurten ryhmän, niin polynomin $f(x)$ kaikki juuret ovat $1, \omega, \omega^2, \ldots, \omega^{n-1}$. Juuret ovat lisäksi erillisiä, sillä ω oletettiin primitiiviseksi n:neksi ykkösenjuureksi, eikä siten voi päteä $\omega^m = 0$ millään $m < n$. Polynomilla $f(x)$ ei siis ole moninkertaisia juuria, eli se on separoituva. Kukin juuri ω^i on alkion ω potenssina laajennuksen $K(\omega)$ alkio, joten polynomi $f(x)$ jakautuu ensimmäisen asteen tekijöihin laajennuksessa $K(\omega)$, sillä se voidaan nyt ilmaista muodossa

$$f(x) = \prod_{j=0}^{n-1} (x - \omega^j).$$

Laajennus $K(\omega)$ on lisäksi pienin laajennus, missä $f(x)$ jakautuu ensimmäisen asteen tekijöihin, sillä minkä tahansa sellaisen laajennuksen on pakko sisältää juuri ω, ja kuitenkin $K(\omega)$ on pienin alkion ω sisältävä laajennus. Laajennus $K(\omega)$ on siis separoituvan polynomin $f(x)$ juurikunta ja siten lauseen 6.4 perusteella Galois.

Osoitetaan vielä, että laajennuksen $K(\omega)/K$ Galois'n ryhmä $\mathrm{Gal}(K(\omega)/K)$ on vaihdannainen. Olkoot $\sigma, \tau \in \mathrm{Gal}(K(\omega)/K)$. Kuvaukset σ ja τ permutoivat polynomin $f(x)$ juuria lauseen 5.2 mukaisesti, joten voidaan merkitä $\sigma(\omega) = \omega^s$ ja $\tau(\omega) = \omega^t$ joillain s, t. Olkoon nyt $\alpha \in K(\omega)$. Lauseen 2.14 nojalla alkio α voidaan esittää muodossa $\alpha = \sum_i k_i \omega^i$, mutta K-automorfismeina σ ja τ kiinnittävät alkiot $k_i \in K$, joten

$$\sigma(\tau(\alpha)) = \sigma\Big(\tau\Big(\sum_i k_i \omega^i\Big)\Big) = \sum_i k_i(\sigma(\tau(\omega^i))) = \sum_i k_i(\sigma(\tau(\omega))^i),$$

missä

$$\sigma(\tau(\omega)) = \sigma(\omega^t) = \sigma(\omega)^t = \omega^{st} = \omega^{ts} = \tau(\omega)^s = \tau(\omega^s) = \tau(\sigma(\omega)).$$

Nyt siis

$$\sigma(\tau(\alpha)) = \sum_i k_i(\sigma(\tau(\omega))^i) = \sum_i k_i(\tau(\sigma(\omega))^i) = \tau\Big(\sigma\Big(\sum_i k_i \omega^i\Big)\Big) = \tau(\sigma(\alpha)),$$

joten ryhmä $\mathrm{Gal}(K(\omega)/K)$ on vaihdannainen. □

Nyt voidaan osoittaa, että primitiivinen n:s ykkösenjuuri varmistaa juurilaajennuksen välilaajennusten olevan Galois'n laajennuksia. Todistuksessa on myös kiinnostava yksityiskohta (7.9), jossa näytetään, että mikä tahansa n:s juurros on mahdollista ilmaista primitiivisen ykkösenjuuren avulla.

Lause 7.8. *Oletetaan, että J/K on n-juurilaajennus, jolla on alikuntien jono*

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = J,$$

missä $K_{i+1} = K_i(\alpha_i)$ jollain sellaisella $\alpha_i \in K_{i+1}$, että $\alpha_i^n \in K_i$. Jos K sisältää primitiivisen n:nen ykkösenjuuren ω, niin laajennuksen J/K jokainen välilaajennus K_{i+1}/K_i on Galois ja jokainen Galois'n ryhmä $\mathrm{Gal}(K_{i+1}/K_i)$ on vaihdannainen.

Todistus. Osoitetaan, että kukin välilaajennus K_{i+1}/K_i on polynomin

$$f_i(x) = x^n - \alpha_i^n \in K_i[x]$$

juurikunta. On huomattava, että vaikka $\alpha_i \in K_{i+1}$, niin polynomi $f(x)$ on silti K_i-kertoiminen, sillä $\alpha_i^n \in K_i$.

Polynomilla $f_i(x)$ on ainakin juuri α_i. Jos $\alpha_i = 0$, niin $K_i(\alpha_i) = K_i$ ja edelleen $K_{i+1}/K_i = K_i/K_i$. Tällaisen laajennuksen Galois'n ryhmän ainut alkio on identtinen kuvaus, joka pitää kunnan K_i paikallaan, joten laajennus $K_{i+1}/K_i = K_i/K_i$ on Galois. Voidaan siis olettaa, että $\alpha_i \neq 0$, jolloin myös $\alpha_i^n \neq 0$, sillä jokainen kunta on myös kokonaisalue.

Olkoon β on jokin toinen polynomin $f_i(x)$ juuri. Tällöin $f(\beta) = \beta^n - \alpha_i^n = 0$, joten $\beta^n = \alpha_i^n$ ja edelleen

$$\left(\frac{\beta}{\alpha_i}\right)^n = 1.$$

Alkio β/α_i on siis n:s ykkösenjuuri, ja siten

$$\frac{\beta}{\alpha_i} = \omega^r$$

jollain r. Mielivaltaiselle juurelle β pätee siis $\beta = \omega^r \alpha_i$ ja toisaalta mikä tahansa alkio muotoa $\omega^j \alpha_i$ on polynomin $f_i(x)$ juuri, joten polynomin $f_i(x)$ juuret ovat

$$\alpha_i,\ \omega\alpha_i,\ \omega^2\alpha_i,\ \ldots,\ \omega^{n-1}\alpha_i \in K_i(\alpha_i). \tag{7.9}$$

Ykkösenjuurten ryhmän alkiot ovat erillisiä, joten kukin polynomin $f_i(x)$ juurista $\omega^j \alpha_i$ on myös erillinen. Polynomi $f_i(x)$ on siis separoituva, ja kaikkien n:n juurensa avulla se voidaan esittää muodossa

$$f_i(x) = \prod_{j=0}^{n-1} (x - \omega^j \alpha_i),$$

joten polynomi $f_i(x)$ jakautuu ensimmäisen asteen termien tuloksi laajennuksessa $K_i(\alpha_i)$. Laajennus $K_{i+1} = K_i(\alpha_i)$ on kuitenkin pienin mahdollinen laajennus, jossa $f_i(x)$ jakautuu ensimmäisen asteen termien tuloksi, sillä jokaisen sellaisen laajennuksen on pakko sisältää juuri α_i, ja $K_i(\alpha_i)$ on pienin juuren α_i sisältävä laajennus. Laajennus $K_i(\alpha_i)$ on siis separoituvan K_i-kertoimisen polynomin $f_i(x)$ juurikunta, joten laajennus $K_i(\alpha_i)/K_i = K_{i+1}/K_i$ on Galois lauseen 6.4 nojalla.

Osoitetaan vielä, että kunkin laajennuksen $K_{i+1}/K_i = K_i(\alpha_i)/K_i$ Galois'n ryhmä on vaihdannainen. Olkoot $\sigma, \tau \in \mathrm{Gal}(K_i(\alpha_i)/K_i)$. Lauseen 2.14 nojalla laajennuksen $K_i(\alpha_i)$ mielivaltainen alkio λ voidaan esittää muodossa $\lambda = \sum_j k_j \alpha_i^j$, ja koska K_i-automorfismit kiinnittävät alkiot $k_j \in K_i$, niin

$$\sigma(\tau(\lambda)) = \sigma\Big(\tau\Big(\sum_j k_j \alpha_i^j\Big)\Big) = \sum_j k_j(\sigma(\tau(\alpha_i^j))) = \sum_j k_j(\sigma(\tau(\alpha_i))^j).$$

Galois'n ryhmän alkiot permutoivat polynomin $f_i(x)$ juuria lauseen 5.2 perusteella, joten voidaan merkitä $\sigma(\alpha_i) = \omega^s \alpha_i$ ja $\tau(\alpha_i) = \omega^t \alpha_i$ joillakin s, t. Kunnan K oletettiin sisältävän alkion ω, joten kaikille ykkösenjuurille ω^r pätee $\omega^r \in K$. Kuvaukset σ ja τ pitävät siis myös ykkösenjuuret paikallaan, joten

$$\begin{aligned}\sigma(\tau(\alpha_i)) &= \sigma(\omega^t \alpha_i) = \omega^t \sigma(\alpha_i) = \omega^t \omega^s \alpha_i = \omega^{t+s} \alpha_i = \omega^{s+t} \alpha_i = \omega^s \tau(\alpha_i) = \tau(\omega^s \alpha_i) \\ &= \tau(\sigma(\alpha_i)).\end{aligned}$$

Nyt siis

$$\sigma(\tau(\lambda)) = \sum_j k_j (\sigma(\tau(\alpha_i))^j) = \sum_j k_j (\tau(\sigma(\alpha_i))^j) = \tau\Big(\sigma\Big(\sum_j k_j \alpha_i^j\Big)\Big) = \tau(\sigma(\lambda)),$$

joten ryhmä $\mathrm{Gal}(K_{i+1}/K_i)$ on vaihdannainen. □

Tarkastellaan lopuksi vielä esimerkkiä Galois'n yhteyden soveltamisesta tilanteessa, jossa juurilaajennus itsessään on Galois. Tällöin Galois'n teorian peruslause liittää välilaajennuksiin normaaleja aliryhmiä, ja aiemmissa todistuksissa saadut vaihdannaiset Galois'n ryhmät puolestaan tuottavat vaihdannaisia tekijäryhmiä. Tutkitaan, voidaanko Galois'n yhteyden avulla löytää jokin Galois'n ryhmän ominaisuus, joka pätee vain juurtamalla ratkeaville polynomeille.

Esimerkki 7.10. Olkoon K kunta, jonka karakteristika on nolla, ja joka sisältää primitiivisen n:nen ykkösenjuuren ω. Oletetaan, että polynomi $f(x) \in K[x]$ on juurtamalla ratkeava, jolloin on siis olemassa juurilaajennus

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = J,$$

missä $K_{i+1} = K_i(\alpha_i)$ jollain sellaisella $\alpha_i \in K_{i+1}$, että $\alpha_i^n \in K_i$ jollain $n \in \mathbb{N}$.

Tutkitaan, millaisen rakenteen laajennuksen J/K Galois'n ryhmä $G = \mathrm{Gal}(J/K)$ saa, jos laajennus J/K on Galois. Peruslauseen 6.7 ensimmäisen kohdan nojalla kutakin välikuntaa K_i vastaa jokin ryhmän G aliryhmä $H_i = \mathrm{Gal}(J/K_i)$, joten voidaan siis määritellä aliryhmien jono

$$G = H_0 \geq H_1 \geq \cdots \geq H_m = \{1\}.$$

Galois'n laajennukseen J/K voidaan soveltaa lausetta 6.4, jonka mukaan kunta J on jonkin separoituvan K-kertoimisen polynomin juurikunta. Kunta K kuitenkin sisältyy jokaiseen välikuntaan K_i, joten tämä samainen separoituva polynomi on myös K_i-kertoiminen, eli laajennus J/K_i on siten Galois. Myös siihen voidaan siis soveltaa peruslausetta. Lauseen 7.8 nojalla kukin laajennuksista K_{i+1}/K_i on Galois, joten peruslauseen toisen kohdan nojalla pätee $H_{i+1} \trianglelefteq H_i$.

Peruslauseen toinen kohta antaa lisäksi $\mathrm{Gal}(K_{i+1}/K_i) \cong H_i/H_{i+1}$. Lauseen 7.8 nojalla kukin Galois'n ryhmä $\mathrm{Gal}(K_{i+1}/K_i)$ on kuitenkin vaihdannainen, joten kukin tekijäryhmä H_i/H_{i+1} on siis myös vaihdannainen. Galois'n ryhmän $\mathrm{Gal}(J/K)$ aliryhmien H_i jono voidaan siis esittää muodossa

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\},$$

missä kukin tekijäryhmä H_i/H_{i+1} on vaihdannainen.

Yllä olevassa esimerkissä löydettiin juurtamalla ratkeavan polynomin juurilaajennuksen Galois'n ryhmän sisältä siis normaalien aliryhmien jono, jonka tekijäryhmät ovat vaihdannaisia. Tähän lopputulokseen päästiin kuitenkin olettamalla ensin primitiivisen n:nen ykkösenjuuren sisältyminen kuntaan K ja sitten olettamalla juurilaajennuksen J/K olevan Galois. Seuraavassa luvussa käsitelläänkin ne tarpeelliset yksityiskohdat, jotka mahdollistavat saman jonorakenteen löytymisen yleisessä tilanteessa, ja annetaan kyseiselle jonorakenteelle sen tärkeyttä kuvaava nimi.

Luku 8

Ratkeavuus

Galois'n läpimurto oli selvittää polynomin ratkeavuus suoraan sen Galois'n ryhmän rakenteesta. Tarvittavaa ryhmän rakennetta kutsutaankin osuvasti ratkeavuudeksi, ja se on juurikin sama normaalien aliryhmien muodostama jonorakenne, joka löydettiin luvun 7 päättäneessä esimerkissä 7.10. Tämän luvun keskeisin tulos onkin lause 8.8, joka osoittaa, että polynomin Galois'n ryhmän ratkeavuus on välttämätön ja riittämätön ehto polynomin juurtamalla ratkeavuudelle.

Aiemmin kuitenkin todettiin, että polynomin Galois'n ryhmä on samaistettavissa jonkin symmetrisen ryhmän tai sen aliryhmän kanssa. Luvussa kuitenkin osoitetaan, että symmetrinen ryhmä S_n ei ole ratkeava, kun $n \geq 5$. Mikäli on siis olemassa viidettä tai sitä korkeampaa astetta olevia polynomeja, joiden Galois'n ryhmä on koko S_n, ei näille polynomeille ole mahdollista muodostaa yleistä ratkaisukaavaa. Luvun päättääkin esimerkki, jossa tutkitaan viidennen asteen polynomia, joka ei ole juurtamalla ratkeava.

8.1 Ryhmän ratkeavuus

Aloitetaan määrittelemällä ratkeavuus täsmällisesti.

Määritelmä 8.1. Ryhmä on *ratkeava*, jos sillä on jono aliryhmiä

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\},$$

missä kukin tekijäryhmä H_i/H_{i+1} on vaihdannainen.

On hyvä huomata, että määritelmän aliryhmien jonossa kukin aliryhmä on vain *seuraavan* aliryhmän normaali aliryhmä. Ratkeavuus ei siis vaadi, että jokainen jonon aliryhmistä olisi myös ryhmän G normaali aliryhmä.

Luvun 7 päättäneessä esimerkissä 7.10 löydettiin ratkeavuuden jonorakenne polynomin Galois'n ryhmän sisältä, mutta yllä oleva määritelmä yleistää ratkeavuuden myös muille ryhmille. Seuraavassa esimerkissä tutkitaan symmetrisen ryhmän S_3 ratkeavuutta, ja pian näytetään täsmällisesti, että symmetrisen ryhmän ratkeavuus nousee avainasemaan polynomien ratkeavuutta tutkittaessa.

Esimerkki 8.2. Symmetrisen ryhmän S_3 alkion (123) virittämä aliryhmä

$$\langle (123) \rangle = \{(1), (123), (321)\}$$

on normaali, sillä Lagrangen lauseen nojalla sen indeksi on 2. Triviaali aliryhmä $\{(1)\}$ on puolestaan aina normaali, joten voidaan muodostaa aliryhmien jono

$$S_3 \trianglerighteq \langle (123) \rangle \trianglerighteq \{(1)\},$$

jolla on tekijäryhmät $S_3/\langle (123) \rangle$ ja $\langle (123) \rangle / \{(1)\}$. Ryhmä $S_3/\langle (123) \rangle$ on kaksialkioisena vaihdannainen, kun taas ryhmä $\langle (123) \rangle / \{(1)\} = \langle (123) \rangle$ on syklinen ja siksi vaihdannainen. Ryhmä S_3 on siis ratkeava.

Ratkeavuuden edellyttämän jonorakenteen löytäminen ei kuitenkaan aina ole helppoa. Usein onkin helpompaa osoittaa ratkeavuus näyttämällä, että tarkasteltava ryhmä on jonkin ratkeavan ryhmän homomorfinen kuva.

Lause 8.3. *Ratkeavan ryhmän homomorfinen kuva on ratkeava.*

Todistus. Olkoon G ratkeava ryhmä, jolloin on siis olemassa aliryhmien jono

$$G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\},$$

missä kukin tekijäryhmä $H_i \trianglerighteq H_{i+1}$ on vaihdannainen. Olkoon $\gamma \colon G \to A$ jokin ryhmähomomorfismi. Tällöin jokaisen aliryhmän H_{i+1} homomorfinen kuva $\gamma(H_{i+1})$ on ryhmän $\gamma(H_i)$ aliryhmä homomorfismin ominaisuuksien perusteella, joten osoitetaan vielä, että tällöin $\gamma(H_i) \trianglerighteq \gamma(H_{i+1})$. Aliryhmien H_i jonon jokaiselle jäsenelle pätee $H_i \trianglerighteq H_{i+1}$, joten kaikilla $a \in H_{i+1}$ ja $x \in H_i$ pätee $xax^{-1} \in H_{i+1}$. Näin ollen $\gamma(xax^{-1}) \in \gamma(H_{i+1})$, ja siten

$$\gamma(xax^{-1}) = \gamma(x)\gamma(a)\gamma(x)^{-1} \in \gamma(H_{i+1}),$$

mistä seuraa $\gamma(H_i) \trianglerighteq \gamma(H_{i+1})$.

Osoitetaan vielä, että kukin tekijäryhmä $\gamma(H_i)/\gamma(H_{i+1})$ on vaihdannainen. Oletetaan, että $\gamma(x), \gamma(y) \in \gamma(H_i)$ joillakin $x, y \in H_i$. Ryhmä on vaihdannainen, jos sen minkä tahansa kahden alkion kommutaattori on ryhmän neutraalialkio, joten tekijäryhmän $\gamma(H_i)/\gamma(H_{i+1})$ tapauksessa riittää osoittaa, että $\gamma(x)\gamma(y)\gamma(x)^{-1}\gamma(y)^{-1} \in \gamma(H_{i+1})$. Kukin

tekijäryhmä H_i/H_{i+1} on ratkeavuuden nojalla vaihdannainen, joten samaa vaihdannaisuuden kriteeriä käyttämällä on oltava $xyx^{-1}y^{-1} \in H_{i+1}$. Näin ollen $\gamma(xyx^{-1}y^{-1}) \in \gamma(H_{i+1})$, mistä seuraa

$$\gamma(xyx^{-1}y^{-1}) = \gamma(x)\gamma(y)\gamma(x)^{-1}\gamma(y)^{-1} \in \gamma(H_{i+1}),$$

mikä oli osoitettava.

On siis löydetty jono aliryhmiä

$$\gamma(G) = \gamma(H_0) \trianglerighteq \gamma(H_1) \trianglerighteq \cdots \trianglerighteq \gamma(H_m) = \{1\},$$

missä kukin tekijäryhmä $\gamma(H_i)/\gamma(H_{i+1})$ on vaihdannainen, joten ryhmä $\gamma(G)$ on ratkeava. □

Lauseen 5.2 yhteydessä todettiin, että Galois'n ryhmän alkiot ovat samaistettavissa permutaatioihin. Galois'n ryhmä on siis jokin symmetrisen ryhmän aliryhmä ja mahdollisesti koko symmetrinen ryhmä S_n. Näin ollen Galois'n ryhmän ratkeavuuden selvittämiseksi ei tarvitse selvittää koko Galois'n ryhmää, kuten esimerkeissä 5.6 ja 6.8 tehtiin: riittää samaistaa Galois'n ryhmä symmetrisen ryhmän tai sen aliryhmän kanssa ja tutkia sen ratkeavuutta.

Nyt voidaan kuitenkin osoittaa, että symmetrinen ryhmä S_n ei kuitenkaan ole ratkeava, kun $n \geq 5$. Todistamista varten tarvitaan ensin aputulos, joka sekin pätee vain, kun $n \geq 5$.

Lemma 8.4. *Olkoon $U \subset S_n$ symmetrisen ryhmän osajoukko, joka sisältää kaikki 3-syklit, ja olkoon $n \geq 5$. Jos osajoukolla U on normaali aliryhmä $N \trianglelefteq U$, jonka tekijäryhmä U/N on vaihdannainen, niin myös N sisältää kaikki 3-syklit.*

Todistus. Sivuutetaan. Tulos on todistettu esimerkiksi teoksessa [1], s. 71. □

Lause 8.5. *Symmetrinen ryhmä S_n ei ole ratkeava, kun $n \geq 5$.*

Todistus. Oletetaan, että ryhmä S_n olisikin ratkeava, kun $n \geq 5$. Tällöin ryhmässä S_n on jono aliryhmiä

$$S_n = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\},$$

missä kukin tekijäryhmä H_i/H_{i+1} on vaihdannainen. Koska $n \geq 5$, niin ryhmä $S_n = H_0$ sisältää kaikki 3-syklit ja lemman 8.4 nojalla myös sen normaali aliryhmä H_1 sisältää kaikki 3-syklit. Mutta nyt tämän samaisen lemman 8.4 perusteella myös H_2 sisältää kaikki 3-syklit, ja vastaavasti päätellen jokainen jonon $S_n = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\}$ aliryhmä sisältää 3-syklit. Näin ollen myös triviaali aliryhmä $\{1\}$ sisältäisi 3-syklit, mikä on kuitenkin mahdotonta. Ryhmä S_n ei siis ole ratkeava, kun $n \geq 5$. □

8.2 Polynomin ratkeavuus

Pian osoitettava lause 8.8 on Galois'n löytämä välttämätön ja riittävä ehto polynomin ratkeavuudelle: polynomi on juurtamalla ratkeava, jos ja vain jos sen Galois'n ryhmä on ratkeava. Lauseen todistuksen ytimessä on peruslauseen 6.7 soveltaminen juurilaajennukseen sellaisella tavalla, että laajennuksen Galois'n ryhmä voidaan osoittaa ratkeavaksi. Peruslauseen sovelluskohteena olevan laajennuksen on kuitenkin oltava Galois, mitä mielivaltainen juurilaajennus ei välttämättä ole. Usein siirrytäänkin tarkastelemaan juurilaajennuksen pienintä normaalia laajennusta, jotta peruslausetta voitaisiin käyttää.

Määritelmä 8.6. Algebrallisen laajennuksen L/K *normaali sulkeuma* on pienin kunnan K normaali laajennus, joka sisältää kunnan L.

Normaalin sulkeuman olemassaoloa ei ole kovin vaikea osoittaa. Algebrallinen laajennus on aina äärellinen, ja esimerkiksi teoksessa [8], s. 108, on osoitettu, että äärellisellä laajennuksella on aina olemassa normaali sulkeuma.

Juurilaajennuksen normaali sulkeuma on itsekin juurilaajennus. Aina voidaan siis huoletta siirtyä tarkastelemaan juurilaajennuksen normaalia sulkeumaa, sillä tällöin ei menetetä juurilaajennukselle ominaista kuntalaajennusten tornia.

Lemma 8.7. *Olkoon J/K jokin n-juurilaajennus ja N sen normaali sulkeuma. Tällöin laajennus N/K on n-juurilaajennus.*

Todistus. Sivuutetaan. Tulos on todistettu esimerkiksi teoksessa [6], s. 149. □

Nyt voidaan osoittaa täsmälleen, milloin polynomi on juurtamalla ratkeava, ja tuoda yhteen kaikki tähän mennessä käsitellyt asiat. Tarvitsemme polynomien ratkeavuuden selvittämiseen kuitenkin vain seuraavan lauseen toista suuntaa, joten vain sen todistus esitetään tässä täsmällisesti. Todistuksen ytimessä on peruslauseen 6.7 soveltaminen, mutta erityisesti myös luvun 7 loppupuolella käsitellyt lauseet tulevat myös tarpeeseen.

Lause 8.8. *Olkoon K kunta, jonka karakteristika on nolla. Polynomi $f(x) \in K[x]$ on juurtamalla ratkeava, jos ja vain jos sen Galois'n ryhmä on ratkeava.*

Todistus. Oletetaan, että polynomi $f(x) \in K[x]$ on juurtamalla ratkeava. Olkoon L polynomin $f(x)$ juurikunta kunnan K suhteen. Osoitetaan polynomin $f(x)$ Galois'n ryhmä $\mathrm{Gal}(L/K)$ ratkeavaksi näyttämällä sen olevan isomorfinen jonkin ratkeavan Galois'n ryhmän kanssa. Rakennetaan tätä varten juurilaajennus, joka on myös Galois, jolloin voidaan käyttää peruslausetta 6.7 muodostamaan ratkeavuuden vaatima normaalien aliryhmien jono. Ratkeavuuden määritelmässä mainittu jono vaatii kuitenkin vaihdannaisia tekijäryhmiä, joten tehdään välilaajennusten Galois'n ryhmistä vaihdannaisia lisäämällä juurilaajennukseen primitiivinen ykkösenjuuri ja käyttämällä sitten lauseita 7.7 ja 7.8.

Polynomi $f(x)$ on juurtamalla ratkeava, joten on olemassa jokin n-juurilaajennus J/K, missä polynomi $f(x)$ jakautuu ensimmäisen asteen tekijöihin. Kunnan K karakteristika on nolla, joten lauseen 7.6 nojalla on olemassa primitiivinen n:s ykkösenjuuri ω jossain kunnan K laajennuksessa. Alkiolle ω pätee $\omega^n = 1 \in J$, joten $J(\omega)/J$ on n-juurilaajennus. Koska myös J/K on n-juurilaajennus, niin $J(\omega)/K$ on n-juurilaajennus.

Laajennus $J(\omega)/K$ ei kuitenkaan välttämättä ole normaali, jolloin peruslausetta 6.7 ei voitaisi käyttää. Siirrytään siis tarkastelemaan juurilaajennuksen $J(\omega)/K$ normaalia sulkeumaa N. Kunnan K karakteristika on nolla, joten lauseen 3.11 nojalla minkä tahansa kunnan N alkion minimipolynomi on separoituva, minkä seurauksena laajennus N/K on separoituva. Koska laajennus N/K on lisäksi normaali, niin lauseen 6.4 nojalla se on Galois. Lemman 8.7 nojalla laajennus N/K on lisäksi n-juurilaajennus, joten on siis olemassa jono kuntia

$$K = K_0 \subset K_1 \subset \cdots \subset K_m = N,$$

missä $K_{i+1} = K_i(\alpha_i)$ jollain sellaisella $\alpha_i \in K_{i+1}$, että $\alpha_i^n \in K_i$. Alkiolle ω pätee kuitenkin $\omega^n = 1 \in K$, joten se voidaan asettaa ensimmäiseksi kuntaan K lisättäväksi alkioksi α_0, jolloin siis $K_1 = K(\omega)$. Näin voidaan tehdä niin kauan kuin muiden alkioiden α_i lisäämisen järjestystä ei muuteta, sillä nyt kullekin alkiolle $\alpha_i \in K_{i+1}$ pätee edelleen $K_{i+1} = K_i(\alpha_i)$ ja $\alpha_i^n \in K_i$.

Pyritään nyt osoittamaan, että laajennuksen N/K Galois'n ryhmä $\mathrm{Gal}(N/K)$ on ratkeava. Merkitään $G_N = \mathrm{Gal}(N/K)$. Peruslauseen ensimmäisen kohdan nojalla kutakin välikuntaa K_i vastaa ryhmän G_N aliryhmä $H_i = \mathrm{Gal}(N/K_i)$, joten on siis olemassa aliryhmien jono

$$G_N = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}.$$

Laajennus N/K on Galois, jolloin se on lauseen 6.4 perusteella jonkin separoituvan K-kertoimisen polynomin juurikunta. Koska kuitenkin $K \subset K_i$, niin N on samalla myös separoituvan K_i-kertoimisen polynomin juurikunta, joten kukin laajennuksista N/K_i on myös Galois. Nyt voidaan siis soveltaa peruslausetta 6.7 laajennukseen N/K_i. Laajennus $K_1/K = K(\omega)/K$ on Galois lauseen 7.7 nojalla, ja kun $i \geq 1$, niin kukin laajennuksista K_{i+1}/K_i on Galois lauseen 7.8 perusteella, joten peruslauseen toisesta kohdasta saadaan $H_{i+1} \trianglelefteq H_i$.

Nyt siis tiedetään, että $H_{i+1} \trianglelefteq H_i$, joten peruslauseen toisesta kohdasta seuraa lisäksi, että

$$\mathrm{Gal}(K_{i+1}/K_i) \cong H_i/H_{i+1}.$$

Lauseiden 7.7 ja 7.8 nojalla kukin Galois'n ryhmä $\mathrm{Gal}(K_{i+1}/K_i)$ on kuitenkin vaihdannainen, minkä seurauksena kukin tekijäryhmä H_i/H_{i+1} on myös vaihdannainen. Ryhmä G_N on siis ratkeava.

Nyt voidaan osoittaa, että ryhmä $\mathrm{Gal}(L/K)$ on ratkeava. Polynomi $f(x)$ oletettiin juurtamalla ratkeavaksi, joten se jakautuu n-juurilaajennuksessa $J \subset N$ ensimmäisen asteen tekijöihin, mutta juurikunta L on kuitenkin pienin kunnan K laajennus, jossa niin tapahtuu. On siis oltava $L \subset J$ ja erityisesti $L \subset N$, joten laajennusta L/K voidaan tarkastella laajennuksen N/K välilaajennuksena. Sovelletaan nyt peruslausetta 6.7 Galois'n laajennukseen N/K. Kunta L oletettiin separoituvan polynomin $f(x)$ juurikunnaksi, joten laajennus L/K on Galois lauseen 6.4 perusteella. Peruslauseen toisesta kohdasta saadaan siten $\mathrm{Gal}(L/K) \trianglelefteq G_N$ ja edelleen

$$\mathrm{Gal}(L/K) \cong G_N/\mathrm{Gal}(N/L).$$

Tekijäryhmä $G_N/\mathrm{Gal}(N/L)$ on kuitenkin ratkeavan ryhmän G_N homomorfinen kuva, kun homomorfismiksi valitaan kanoninen surjektio

$$\pi\colon G_N \to G_N/\mathrm{Gal}(N/L), \quad \pi(g) = g + \mathrm{Gal}(N/L),$$

joten ryhmä $G_N/\mathrm{Gal}(N/L)$ on siis itsekin ratkeava lemman 8.3 nojalla. Aiemmin kuitenkin todistettiin, että ryhmät $G_N/\mathrm{Gal}(N/L)$ ja $\mathrm{Gal}(L/K)$ ovat isomorfiset, joten myös ryhmä $\mathrm{Gal}(L/K)$ on ratkeava.

Todistuksen toinen suunta esitetään tässä vain luonnostelmana sen vaatimien teknisten yksityiskohtien vuoksi (todistus on esitetty täsmällisesti esimerkiksi teoksessa [6], s. 151). Oletetaan, että polynomin $f(x)$ Galois'n ryhmä $\mathrm{Gal}(L/K)$ on ratkeava. Tällöin on siis olemassa jono aliryhmiä

$$\mathrm{Gal}(L/K) = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_m = \{1\},$$

joilla on vaihdannaiset tekijäryhmät H_i/H_{i+1}. Merkitään $F_i = \mathrm{Fix}(H_i)$. Lauseen 5.12 perusteella $H_i = \mathrm{Gal}(L/F_i)$ ja lisäksi tiedetään $H_i \trianglerighteq H_{i+1}$, joten kukin laajennus F_{i+1}/F_i on peruslauseen 6.7 toisen kohdan mukaan Galois.

Olkoon $M_i = F_i(\omega)$. Voidaan osoittaa, että kukin laajennuksista M_{i+1}/M_i on Galois ja että jokainen Galois'n ryhmä $\mathrm{Gal}(M_{i+1}/M_i)$ on isomorfinen jonkin ryhmän $\mathrm{Gal}(F_{i+1}/F_i)$ aliryhmän kanssa. Näin menetellen voidaan myös osoittaa, että kukin laajennuksista M_{i+1}/M_i on juurilaajennus. Tällöin M_m/K on juurilaajennus, jossa polynomi $f(x)$ jakautuu ensimmäisen asteen tekijöihin, sillä $L = F_m \subset M_m$. Polynomi $f(x)$ on siis juurtamalla ratkeava. □

Teoksessa [12], s. 169, on osoitettu, että symmetrinen ryhmä S_n on ratkeava, kun $n < 5$. Yllä olevan lauseen 8.8 nojalla kaikki astetta $n \leq 4$ olevat polynomit ovat siis juurtamalla ratkeavia, sillä niistä kunkin Galois'n ryhmä on symmetrisen ryhmän S_n aliryhmä. Mutta samasta syystä polynomit, joiden aste on $n \geq 5$, eivät ole juurtamalla ratkeavia, sillä lauseessa 8.5 osoitettiin, että symmetrinen ryhmä S_n ei tällöin ole ratkeava. Viidettä ja

sitä korkeampaa astetta oleville polynomeille ei siis ole mahdollista muodostaa yleistä ratkaisukaavaa.

Rationaalikertoimisten polynomien ratkeamattomuuden havainnollistamiseksi riittääkin siis löytää jokin viidennen asteen polynomi, jonka Galois'n ryhmä on koko symmetrinen ryhmä S_5. Osoitetaan, että mikä tahansa rationaalikertoiminen viidennen asteen polynomi, jolla on tasan kaksi imaginäärijuurta, täyttää tämän ehdon. Ensin tarvitaan kuitenkin aputulos.

Lemma 8.9. *Syklit* (12) *ja* $(12\cdots n)$ *virittävät symmetrisen ryhmän* S_n.

Todistus. Sivuutetaan. Tulos on todistettu esimerkiksi teoksessa [8], s. 131. □

Lause 8.10. *Olkoon* $f(x) \in \mathbb{Q}[x]$ *jaoton viidennen asteen polynomi. Jos polynomilla* $f(x)$ *on tasan kaksi imaginäärijuurta, niin polynomin* $f(x)$ *Galois'n ryhmä on symmetrinen ryhmä* S_5.

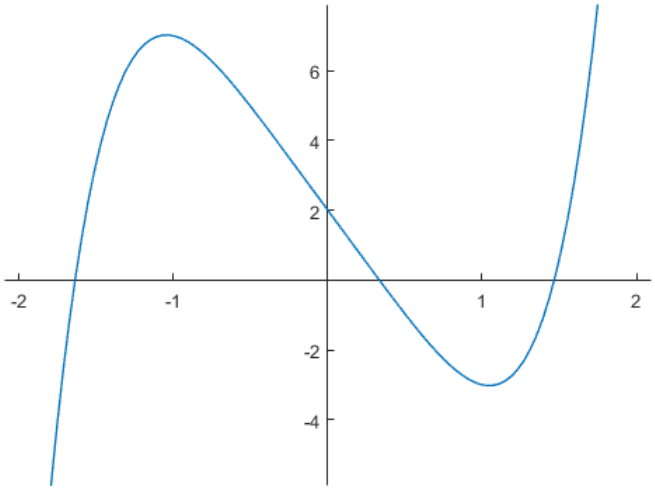
Todistus. Algebran peruslauseen nojalla polynomin $f(x)$ kaikki juuret ovat kunnassa $\mathbb{C}$, joten kunta $\mathbb{C}$ sisältää myös polynomin $f(x)$ juurikunnan L. Merkitään $G = \mathrm{Gal}(L/\mathbb{Q})$. Lauseen 5.2 nojalla tiedetään, että ryhmän G alkiot permutoivat polynomin $f(x)$ juuria. Kunnan $\mathbb{Q}$ karakteristika on nolla, joten lauseen 3.11 nojalla polynomi $f(x)$ on separoituva ja sillä on siten viisi erillistä juurta. Ryhmä G on siis symmetrisen ryhmän S_5 aliryhmä.

Polynomi $f(x)$ on jaoton, joten kunkin sen juuren minimipolynomin asteen on lauseen 2.12 perusteella oltava sama kuin polynomin $f(x)$ asteen eli 5. Nyt lauseen 2.16 perusteella millä tahansa polynomin $f(x)$ juurella $\alpha_i \in L$ siis pätee $[\mathbb{Q}(\alpha_i) : \mathbb{Q}] = 5$. Lausetta 2.5 soveltamalla saadaan

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_i)][\mathbb{Q}(\alpha_i) : \mathbb{Q}] = [L : \mathbb{Q}(\alpha_i)] \cdot 5,$$

joten laajennuksen $L/\mathbb{Q}$ aste $[L : \mathbb{Q}]$ on jaollinen luvulla 5. Lauseen 5.12 perusteella ryhmän G kertaluvulle pätee kuitenkin $|G| = [L : \mathbb{Q}]$, joten myös ryhmän G kertaluku on jaollinen luvulla 5. Näin ollen laajennuksen $L/\mathbb{Q}$ Galois'n ryhmässä G on oltava jokin alkio, jonka kertaluku on 5 (tämä Cauchy'n lauseena tunnettu tulos on todistettu esimerkiksi teoksessa [8], s. 136). Aiemmin todettiin, että ryhmän G alkiot ovat ryhmän S_5 alkioita, ja jokainen ryhmän S_5 alkio voidaan esittää erillisten syklien tulona. Kunkin ryhmän S_5 alkion kertaluku on näiden erillisten syklien pituuksien pienin yhteinen monikerta, joten kertaluvun 5 aliryhmän virittäjä ei voi olla mikään muu kuin 5-sykli. Ryhmässä G on siis oltava jokin 5-sykli.

Muodostetaan nyt lausetta 4.6 käyttäen kuvaus $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$, $\sigma(i) = -i$. Polynomilla $f(x)$ on tasan kaksi imaginäärijuurta, joten ne ovat väistämättä toistensa kompleksikonjugaatit. Kuvaus σ vaihtaa siis polynomin $f(x)$ kahden imaginäärijuuren paikkaa



Kuva 8.1: Polynomifunktio $f(x) = x^5 - 6x - 2$.

keskenään, mutta pitää loput kolme reaalista juurta paikallaan. Toisin sanottuna kuvaus σ on transpositio eli ryhmään G sisältyvä 2-sykli.

Merkitään $\sigma = (12)$. Aiemmin löydetty 5-sykli voidaan esittää muodossa $(12\cdots5)$ merkitsemällä syklin muita alkioita sopivasti ja siirtymällä tarvittaessa tarkastelemaan jotain 5-syklin monikertaa. Näin ollen ryhmässä G on siis syklit (12) ja $(12\cdots5)$, joten lemman 8.9 perusteella on oltava $G = S_5$. □

Esimerkki 8.11. Olkoon $f(x) = x^5 - 6x - 2 \in \mathbb{Q}[x]$. Polynomi $f(x)$ on jaoton Eisensteinin kriteerin perusteella, joten koska kunnan $\mathbb{Q}$ karakteristika on nolla, niin polynomilla $f(x)$ on lauseen 3.11 nojalla viisi erillistä juurta. Tutkimalla polynomin $f(x)$ kuvaajaa (kuva 8.1) huomataan, että juurista kolme on reaalisia, joten sillä on oltava lisäksi tasan kaksi imaginäärijuurta. Nyt lauseen 8.10 perusteella polynomin $f(x)$ Galois'n ryhmä on siis koko symmetrinen ryhmä S_5. Ryhmä S_5 ei kuitenkaan lauseen 8.5 perusteella ole ratkeava, joten lauseen 8.8 nojalla polynomi $f(x)$ ei ole juurtamalla ratkeava.

Kirjallisuutta

[1] Artin, Emil 1942/1998: *Galois Theory.* Dover Publications Inc., New York.

[2] Boyer, Carl B. 1968/1994: *Tieteiden kuningatar, Matematiikan historia, osa II.* Suomentanut Kimmo Pietiläinen. WSOY.

[3] Halmos, Paul R. 1942/1958: *Finite-Dimensional Vector Spaces.* D. van Nostrand Company, Inc., New York.

[4] Häsä, Jokke 2010: *Algebra II.* Luentomoniste, Helsingin yliopisto. `https://www.cs.helsinki.fi/u/jhasa/kurssit/algebraII/materiaali.pdf`

[5] Häsä, Jokke & Rämö, Johanna 2012: *Johdatus abstraktiin algebraan.* Gaudeamus Helsinki University Press.

[6] Morandi, Partick 1996: *Field and Galois Theory.* Springer-Verlag New York Inc., New York.

[7] Pinter, Charles C. 1982: *A Book of Abstract Algebra.* McGraw-Hill Inc.

[8] Stewart, Ian 1973: *Galois Theory.* Chapman and Hall Ltd., London.

[9] Suominen, Kalevi 2004: *Algebra II.* Luentomoniste, Helsingin yliopisto.

[10] Tignol, Jean-Pierre 2001/2011: *Galois' Theory of Algebraic Equations.* World Scientific Publishing Co. Pte. Ltd.

[11] Warner, Seth 1965/1990: *Modern Algebra.* Dover Publications Inc., New York.

[12] Weintraub, Steven H. 2006: *Galois Theory.* Springer Science+Business Media Inc., New York.